Risikovurderinger i forbindelse med outsourcing av informasjons- og kommunikasjonsteknologi (IKT) i petroleumssektoren.

Sissel Ertenstein & Silje Avlesen Løfgren

Vår 2018

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i samfunnssikkerhet SAMMAS / MSAMAS	Vårsemesteret, 2018 **Åpen** / ~~Konfidensiell~~
Forfattere: Sissel Ertenstein & Silje Avlesen Løfgren	…… (signatur forfattere)

Fagansvarlig: Ole Andreas Hegland Engen

Veileder(e): Ole Andreas Hegland Engen

Tittel på masteroppgaven:
Risikovurderinger i forbindelse med outsourcing av informasjons- og kommunikasjonsteknologi (IKT) i petroleumssektoren.

Engelsk tittel:
Risk assessment regarding outsourcing of information and communication technology (ICT) in the Norwegian petroleum sector.

Studiepoeng: 30 stp.

Emneord: Samfunnssikkerhet, petroleumssektoren, outsourcing, IKT, informasjons- og kommunikasjonsteknologi, IKT-sikkerhet, informasjonssikkerhet, risikostyring, risikovurdering, beslutning, styring, læring.	Sidetall: 82 + vedlegg/annet: 2 Stavanger, 28.05.18

Forord

Denne masteravhandlingen er skrevet som en avsluttende del av masterstudiet i samfunnssikkerhet ved universitetet i Stavanger. De siste årene har vært utfordrende, lærerike og spennende. Vi har utviklet oss faglig, og blitt kjent med mange flotte forelesere og medstudenter. Nå runder vi av med en avhandling om IKT-sikkerhet, som er et svært dagsaktuelt og viktig tema for både bransjen og samfunnet.

Først vil vi rette en stor takk til vår veileder Ole Andreas Engen. Takk for alle konstruktive tilbakemeldinger og faglige diskusjoner gjennom prosessen. Dette har vært uvurderlig, og har motivert oss gjennom prosessen. Videre vil det rettes en takk til samtlige informanter som har tatt seg tid til å dele deres erfaringer og kunnskap i deres travle hverdag. Til slutt vil vi rette oppmerksomhet mot våre familier som har holdt ut med oss dette halvåret, og som har oppmuntret oss gjennom lange og travle dager. Tusen takk!

Studien er skrevet i et samarbeid.

28.05.2018

Sissel Louise Beck Ertenstein & Silje Avlesen Løfgren

Sammendrag

Norsk petroleumssektor har de senere år stått ovenfor en digitaliserings- og endringsprosess, som har ført til mer komplekse og integrerte IKT-løsninger. Dette kan føre til økende grad av outsourcing, grunnet krav om kostnadseffektivitet. Dette øker imidlertid risikoen for uønskede hendelse, som følge av et forverret risikobilde. Studien belyser hvordan operatører på norsk sokkel benytter risikovurderinger ved outsourcing av informasjons- og kommunikasjonsteknologi. Dette omfatter hvilke forhold som påvirker operatørenes beslutninger om å tjenesteutsette hele eller deler av IKT-porteføljen til eksterne tjenesteleverandører. Studien inkluderer eksperters forståelse av risiko og sårbarhet, samt faktorer i omgivelsene og sektoren som påvirker operatørenes beslutninger vedrørende outsourcing. Det er en eksplorativ casestudie, basert på semi-strukturerte intervjuer med eksperter i operatørselskap og Petroleumstilsynet (Ptil), kombinert med fagkunnskap fra dokumenter. Følgende problemstilling er belyst:

«*På hvilken måte benytter operatører risikovurderinger i forbindelse med outsourcing av informasjons- og kommunikasjonsteknologi, og hvilke forhold påvirker ekspertenes vurderinger?*»

Ekspertene trekker fram flere risikofaktorer forbundet med outsourcing, der kulturelle forhold og omdømme er faktorer som vektlegges betydelig i risikovurderingene. Imidlertid er det indikasjoner på at risikoen ikke tilstrekkelig forstås, med tanke på kausalitet, kompleksitet og gjensidig avhengighet. Flere eksperter legger mer vekt på fordeler relatert til økonomi og drift, heller enn risikoene, der bevisstheten rundt egen ansvarsrolle er svak. Samtidig opplever mange av operatørene et press fra deres internasjonale selskap som påvirker deres autonomi. Flere av forholdene kan skyldes mangelfulle risikovurderinger, som kan resultere i et utilstrekkelig risikobilde. Operatørene er imidlertid god på intern læring, selv om det kan legges til rette for mer samhandling mellom virksomheter og myndigheter.

Regelverket i forbindelse med IKT-sikkerhet i sektoren er veldig generelt, som gjør at det er en svak styring fra myndighetene. Dette fører blant annet til at de forholdene Ptil fokuserer på får tilsvarende fokus hos operatørene. Dersom man sammenlikner informasjonssikkerhet i petroleumssektoren mot andre sektorer, eksempelvis helse, finans og kraft, er det tydelige

forskjeller i regelverk. Det er således lite bevissthet og eierskap til egne verdier hos operatørene, som i kombinasjon med et funksjonelt regelverk har en betydning i eksperters risikovurdering- og forståelse.

Helhetsbildet viser at ekspertenes risikoforståelse påvirkes av flere forhold, både risiko, interne og eksterne faktorer, i tillegg til sektorens rammer. Flere av studiens funn er i tråd med tidligere forskning og fagdokumenter. Enkelte funn som uklare ansvarsforhold og svak risikostyring fra myndighetsnivå er av vesentlig betydning for både hvordan og hvorfor man outsourcer. Totaliteten illustrerer at beslutninger om outsourcing tas basert på et utilstrekkelig risikobilde, som potensielt kan ha negative konsekvenser både for den enkelte ekspert, operatør, sektor og samfunnet generelt.

Abstract

In recent years, the Norwegian petroleum sector has faced a digitalization- and change process, which has led to more complex and integrated ICT solutions. This can lead to an increasing degree of outsourcing, due to demands for cost-effectiveness. However, this increases the risk of undesired events, due to a deteriorated risk image. This study examines how operators on the Norwegian shelf use risk assessments in outsourcing of information and communication technology. This includes what conditions affect operators´ decision to outsource all or parts of the ICT-portfolio to external service providers. The study also includes experts´ understanding of risk and vulnerability, as well as factors in the environment and the sector that affect operators´ decisions regarding outsourcing. This is an exploratory case study based on semi-structured interviews with experts in operating companies and the Petroleum safety authority (PSA), combined with professional knowledge gathered from documents. The following problem is highlighted:

«In what way are risk assessments regarding outsourcing of information and communication technology in the petroleum sector used, and which conditions affect the experts´ assessments?»

The experts point out several risk factors associated with outsourcing, where cultural relationships and reputation are significant emphasized in the risk assessments. However, there are indications that the risk is not sufficiently understood, given the causality, complexity and mutual dependence. Several experts emphasize benefits related to economics and operation, instead of the risks, where the awareness of their own responsibility is weak. At the same time, many of the operators are experiencing pressure from their international companies that affect their autonomy. Several of the conditions may be due to insufficient risk assessments, which may result in an insufficient risk image. However, the operators´ are good at internal learning, although it is possible to facilitate more interaction between the companies and authorities.

The regulatory framework in the field of ICT security in the sector is very general, that means there is a weak government control. This leads to that the conditions PSA´s focuses on gets corresponding focus of the operators. Comparing information security in the petroleum sector towards other sectors, such as health, finance and power, there are distinct differences in regulatory

frameworks. Thus, there is little awareness and ownership of own values at the operators, which in combination with a functional framework has an impact on experts´ risk assessment and understanding.

The overall picture shows that experts´ perceptions of risk are influenced by several factors, both risk, internal and external factors, in addition to the sector's framework. Several of the findings in the study are in line with previous research and academic papers. Certain findings such as unclear responsibilities and weak governmental risk management are essential for both how and why companies outsource. In total, this illustrates that outsourcing decisions are based on an insufficient risk image that potentially may have negative consequences for the individual expert, operator, sector and society in general.

Innholdsfortegnelse

Tabelliste.

1. Innledning

Outsourcing av informasjons- og kommunikasjonsteknologi (IKT) er en trend som utvikler seg i et hurtig tempo og i ulike former (Qi & Chau, 2012). Stadig flere virksomheter velger å outsource hele eller deler av deres IKT-tjenester til eksterne leverandører, blant annet på grunn av globalisering, kostnadseffektive fordeler, økt sikkerhet og mer stabile tjenester (Dhillon, Syedb & de Sá-Soaresc, 2017; Wei & Peach, 2006). I Norge gjelder dette et økende antall offentlige så vel som private virksomheter, der stadig flere outsourcer til lavkostnadsland som Øst-Europa, Kina eller India (Kommunal- og moderniseringsdepartementet, 2015; Nassimbeni, Sartor & Dus, 2012). Imidlertid er outsourcing svært vanskelig på grunn av mange og komplekse risikofaktorer, og mange prosesser mislykkes (Dhillon et al., 2017; Liu, Zhang, Keil & Chen, 2010; Qi & Chau, 2012).

I Norge har beslutninger om outsourcing fått stor oppmerksomhet i media. Dette er spesielt fordi Statoil, Helse Sør-Øst og Broadnet møtte en rekke utfordringer ved å sette ut IKT-tjenester til lavkostnadsland. Som følge av dette har alle blitt rammet av mange uheldige hendelser, med mer eller mindre alvorlige konsekvenser (Ekroll, Bjerkan & Olsen, 2017; NSM, 2017b; Tomter, Remen & Wernersen, 2017). Også i Sverige ble svært sensitiv informasjon kompromittert, noe som nesten veltet den svenske regjeringen (Jacobsen, 2017). Hendelsene belyser risikoen som outsourcing fører med seg, der det viser seg å være spesielt vanskelig å ha kontroll over tilgang til systemer og sensitiv informasjon. Et fellestrekk er at IT-arbeidere hos tjenesteleverandører har hatt uautorisert tilgang til systemer og/eller informasjon (Ekroll et al., 2017; Tomter & Remen, 2017; Tomter et al., 2017). Jacobsen (2017) karakteriserer outsourcing som «*sikkerhet på anbud*», og mener digitaliseringen skaper store sikkerhetsbrister, der sikkerheten blir tilsidesatt for rimeligere drift.

Å vurdere risikoen som outsourcing fører med seg kan være avgjørende. Dette fordi risikoen for uønskede hendelser er høy og konsekvensene kan være alvorlig, mye på grunn av forlengede verdikjeder som øker sårbarheten og kompleksiteten. Samtidig er det stadig flere forsøk på å få tilgang til systemer og informasjon gjennom målrettede angrep mot underleverandører (NSM, 2017b). Dette understreker et behov for grundig vurdering av risiko før virksomheter beslutter å outsource, for å sikre at sikkerhetsmålene konfidensialitet, integritet og tilgjengelighet ikke

kompromitteres. Imidlertid viser det seg at virksomheter gjennomfører utilstrekkelige risikovurderinger, om de i det hele tatt gjennomføres, i forkant av beslutninger om å sette ut IKT-tjenester (NSM, 2017b). Denne utfordringen gjenspeiles i alle hendelsene. Dels kan det handle om utfordringer når det gjelder å etablere en god forståelse for hvilken risiko og sårbarhet som er knyttet til IKT, og dels vansker med analyse av risikoer (Selvik, 2017). Dette er således en motivator og danner grunnlag for denne studien, med utgangspunkt i å forstå hvordan operatører vurderer risiko ved outsourcing. Videre søkes det å se på hvordan risikovurderinger legger grunnlag for å ta gode beslutninger. Med bakgrunn i hendelsene som har inntruffet, er dette et fenomen som er svært dagsaktuelt og fører med tverrsektorielle problemstillinger.

1.1 Bakgrunn for studien

Outsourcing, også kjent som tjenesteutsetting, er en økende trend i de fleste sektorer. Petroleumssektoren i Norge er i endringsprosesser knyttet til krav om kostnadseffektivitet og omstilling til digitale løsninger. De industrielle kontrollsystemene er i stor grad digitalisert og avhengig av digital teknologi, og kan dermed benevnes som IKT-systemer. Omstillingsprosessene fører til at IKT-tjenester og/eller drift i større grad kan bli outsourcet til eksterne leverandører (DNV GL, 2018; IRIS, 2018). Både effektivisering og teknologiutviklingen fører imidlertid til endring i risikobildet. Aktiviteter i sektoren er forbundet med høy risiko, som i økende grad vil være forårsaket av nye digitale trusler og sårbarheter - både som følge av intenderte og uintenderte hendelser. Eksplosjonen i oljerørledningen i Erzincan og Deepwater Horizon-ulykken er eksempler på dette (Forsvarets forskningsinstitutt, 2016; NOU 2015:13). Det er bekymringsverdig at det stadig blir vanskeligere å beskytte systemer, og spesielt er leverandøravhengighet med hensyn til uønskede hendelser fremtredende (IRIS, 2018). Samtidig er det forventet at hyppigheten og konsekvensene av IKT-hendelser vil øke i årene fremover, og det krever økt fokus på forbedring når det gjelder IKT-sikkerhet i petroleumssektoren (Arbeids- og sosialdepartementet, 2018; NSM, 2017a). Utfordringer som følger outsourcing innebærer situasjonsforståelse og risikopersepsjon, der utvidelse og integrasjon av ulike IKT-systemer krever ny systemforståelse (IRIS, 2018).

Det er få sektorer som virker forberedt på å håndtere nye trusler. I petroleumssektoren karakteriseres IKT-sikkerheten som «full av svakheter», og systemene som sårbare (Elvevold, 2018). Virksomheter er selv ansvarlig for egen IKT-sikkerhet, blant annet med tanke på å kartlegge

og lukke sårbarheter (Justis- og beredskapsdepartementet, 2016a; NSM, 2017b). Outsourcing av IKT krever dermed god risikostyring (Frost, 2000), som bør være integrert i virksomhetenes prosesser (NSM, 2017b). Det har derimot vist seg at virksomheter er sårbare grunnet mangelfull sikkerhetsstyring og risikovurderinger ved outsourcing. Dette er vesentlig å gjennomføre i forkant, for å kunne ta velinformerte beslutninger og ivareta sikkerheten til IKT-tjenestene som settes ut. I enkelte tilfeller stiller lovverket krav til dette, eksempelvis i helse-, finans- og kraftsektoren (Direktoratet for e-helse, 2016), mens det i petroleumssektoren er mer fragmenterte regelverk i forbindelse med IKT-sikkerhet (DNV GL, 2015; NUPI, 2018). I tillegg har Petroleumstilsynet (Ptil) blitt kritisert for manglende tilsyn med hensyn til IKT-sikkerhet (Riksrevisjonen, 2017). På bakgrunn av sektorens betydning for samfunnet er risikostyring i forbindelse med outsourcing i petroleumssektoren en interessant tematikk, selv om det er en sektorovergripende problemstilling.

1.1.1 Formål og problemstilling

Formålet med studien er å undersøke hvordan operatører i petroleumssektoren benytter risikovurderinger i forbindelse med outsourcing av IKT, og hva som påvirker vurderingene. Det søkes i den forbindelse å undersøke hvordan eksperter forstår og vektlegger risiko og sårbarhet, og hvilke faktorer som påvirker virksomhetenes/operatørene risikovurderinger.

Følgende problemstilling er utarbeidet:
«*På hvilken måte benytter operatører risikovurderinger i forbindelse med outsourcing av informasjons- og kommunikasjonsteknologi, og hvilke forhold påvirker ekspertenes vurderinger?*»

For å besvare problemstillingen er følgende forskningsspørsmål utarbeidet:

(i) *Hvordan forstår eksperter risiko og sårbarhet knyttet til outsourcing, og hvordan vektlegges dette i risikovurderinger?*

(ii) *I hvilken grad har interne og eksterne faktorer betydning for operatørers vurderinger vedrørende outsourcing?*

(iii) *Hvordan påvirker læring og styring i sektoren operatørenes vurderinger når det gjelder informasjonssikkerhet?*

For å besvare problemstillingen er det først en søken etter hvordan eksperter forstår og vektlegger risiko og sårbarhet i vurderinger vedrørende outsourcing av IKT. Eksperters risikoforståelse kan være av betydning for hvorvidt operatører beslutter å outsource. En ekspert forstås her som en som arbeider innen IKT i et operatørselskap, og har kjennskap til og/eller deltatt i risikovurderinger knyttet til outsourcing. I denne sammenheng innebærer risikovurderinger ikke nødvendigvis bare fullverdige risikoanalyser, men alle vurderinger som operatørene gjør med hensyn til outsourcing. Det er videre en relasjon mellom risikovurderingsprosesser og forhold i virksomhetenes omgivelser (Prado, 2011). På bakgrunn av dette er det valgt å undersøke hvorvidt interne og/eller eksterne faktorer kan ha innvirkning på vurderingene som gjennomføres av operatørene. Spesielt fordi tekniske, organisatoriske og interorganisatoriske faktorer bør inkluderes og kan være av betydning (NOU 2015:13). Da sektorielle forhold kan legge føringer for virksomheters prosesser og valg (Prado, 2011), er det avslutningsvis rettet et fokus på hvorvidt læring og styring i sektoren påvirker eksperters forståelse av risiko og operatørenes vurdering ved outsourcing. Det er tidligere påpekt blant annet manglende styring i sektoren når det gjelder IKT-sikkerhet, og derav er det relevant å undersøke om dette er av betydning for operatørenes handlingsvalg. Da digitalisering kan medføre tverrsektorielle problemstillinger (NOU 2015:13), vil slike utfordringer belyses med eksempler fra andre sektorer der det anses hensiktsmessig. Således søkes det å reflektere over relevante sektoruavhengige problemstillinger ved å se de i et større perspektiv. Forskningsspørsmålene tar for seg elementer som sammen utgjør en helhet av vurderingene som ekspertene bør legge til grunn når vurderer og/eller tar beslutninger om outsourcing av IKT-tjenester.

1.2 Avgrensning

Outsourcing av IKT-tjenester fører med tverrsektorielle problemstillinger som ikke kan løses alene (Kommunal- og moderniseringsdepartementet, 2015). Imidlertid er det valgt å avgrense studien til operatører i petroleumssektoren på norsk sokkel. Dette er på bakgrunn av økt sårbarhet i IKT-systemene som et resultat av større integrasjon av systemer, og komplekse verdikjeder grunnet leverandøravhengigheter (IRIS, 2018; NOU 2015:13). Videre er sektoren stadig mer utsatt for digitale trusler (NUPI, 2018), samtidig som det er antydninger på sårbare datasystemer, fragmenterte regelverk og uklare ansvarsforhold når det gjelder IKT-sikkerhet (DNV GL, 2015; Elvevold, 2018).

1.3 Tidligere forskning

Det finnes mye forskning innen outsourcing av IKT-tjenester, der store deler er av internasjonal karakter. Dette er fordi andre land, spesielt USA og Kina, outsourcer mye når det gjelder IKT (Liu et al., 2010; Tafti, 2005). I Norge er forskningen i stor grad rettet mot finanssektoren og ledelse ved outsourcing (Gottschalk, 2005a; Gottschalk, 2005b). Tidligere internasjonal forskning belyser risikoer ved fenomenet omstendelig. På bakgrunn av dette anses det hensiktsmessig å benytte dette, da studien søker å forstå vurderinger ved outsourcing. I tillegg er flere risikoer som følge av digitalisering uavhengig av tid og geografisk område, noe som forsterkes av outsourcing. Der forskning berører juridiske forhold, spesielt etterlevelse av krav i henhold til lovverk, vil det ikke kunne trekkes direkte paralleller, men heller ses på som en viktig faktor som må tilpasses norsk lovverk.

Globalisering er en av hovedårsakene til det økte behovet for å tjenesteutsette IKT-tjenester blant virksomheter. Mye av forskningen understreker fordelene som outsourcing medfører, der blant annet tilgang til kompetanse, fokus på kjerneaktiviteter, kostnadseffektivitet og økende konkurranse ofte er av betydning for hvorfor virksomheter outsourcer (Dhillon et al., 2017; Fan, Suo & Feng, 2012). Imidlertid belyser en betydelig mengde av forskningen risikofaktorer knyttet til outsourcing (Dhillon et al., 2017; Fan et al., 2012; Lui et al., 2010; Prado, 2011; Wu, Fung, Feng & Wang, 2017), og flere har i forskningsbidrag utviklet ulike risikoanalyser eller rammeverk for å identifisere og håndtere risikoen (Aris, Arshad & Mohamed, 2008; Doomun, 2008; Lui et al., 2010; Nassimbeni et al., 2012; Prado, 2011; Wei & Peach, 2006). En av de største utfordringene ved outsourcing av IKT er likevel risikovurderinger, spesielt på grunn av at informasjonssikkerhet er blitt en signifikant risiko ved at det er vanskelig å ha kontroll. Både grunnet kompleksiteten i systemene, men også oppfølgingskontroll på tjenesteleverandør (Fan et al., 2012; Khalfan, 2004; Lacity et al., 2010). Det som er bekymringsverdig er at informasjonssikkerheten trues av risikoer innen ulike kategorier, der disse strekker seg fra teknologiske til organisatoriske. Konfidensialitet, integritet og tilgjengelighet er noe av det mest kritiske ved outsourcing, og må vektlegges i vurderinger (Dhillon et al., 2017; Goodman & Ramer, 2007). Generelt bidrar mye av litteraturen til en god basis for å forstå fordelene og ulempene ved outsourcing, i tillegg til flere bidrag med ulike rammeverk for å håndtere risikoen.

Denne studien søker å forstå hvordan operatører benytter risikovurderinger, og hvilke forhold som påvirker risikovurderingene. Risikopersepsjon er et viktig bidrag, fordi eksperters forståelse av risiko inkluderes. Det eksisterer forskning innenfor temaet, der blant annet Prado (2011) ser på forholdet mellom risiko og organisasjonskarakteristikk, og Lui et al. (2010) sammenlikner prosjektledere og lederes risikopersepsjon knyttet til outsourcing av IKT. Denne studien vil bidra til å belyse et fenomen med en sektorovergripende problemstilling. Studien fokuserer på petroleumssektoren grunnet digitaliseringen av sektoren (IRIS, 2018), men dette er samtidig en økende trend på samtlige samfunnsnivåer. Studien søker en helhetlig forståelse for hvilke faktorer som påvirker vurderingene som ligger til grunn, som er interessant ettersom risikoer ved outsourcing er veldokumentert. Det er interessant å se på hvordan disse innvirker på vurderingsprosessen hos operatørene, der dette er en tilnærming som ikke er studert tidligere.

1.4 Studiens videre oppbygning

I første kapittel er grunnlaget for studien presentert, der formålet er å undersøke hvordan risiko forstås og vurderes når det gjelder outsourcing av IKT-tjenester i petroleumssektoren. I den sammenheng er det gjennomgått studiens avgrensning og tidligere forskning på feltet.

Videre vil kapittel to utgjøre en redegjørelse for fenomenet outsourcing, samt en kort utgreiing om sentrale begreper som informasjons- og kommunikasjonsteknologi og informasjonssikkerhet.

Kapittel tre innebærer en gjennomgang av teoretiske perspektiver på risikostyring og risikovurderinger, der flere sentrale elementer knyttet til dette blir inkludert.

I kapittel fire presenteres studiens forskningsdesign og metodiske tilnærming, og inkluderer en refleksjon over de valg og vurderinger som tas underveis.

Kapittel fem presenterer studiens resultater i en empirisk fremstilling, strukturert etter forskningsspørsmålene som ble redegjort i første kapittel. Kapittel seks innebærer en diskusjon av resultatene i lys av studiens teoretiske utgangspunkt, for å vurdere hvordan forskningsspørsmålene satt sammen kan besvare gitt problemstilling. Kapittel syv utgjør en konklusjon.

2. Kontekst

Følgende kapittel utgjør rammene til studien. Det vil først redegjøres kort for fenomenet outsourcing, etterfulgt av betydningen av informasjons- og kommunikasjonsteknologi og informasjonssikkerhet. Videre vil rammeverket for IKT-sikkerhet i petroleumssektoren presenteres, med det formål å klargjøre hva operatører må forholde seg til. Avslutningsvis vil det være et fokus på fordeler og risiko, samt hendelser som har inntruffet, som følge av outsourcing av IKT-tjenester.

2.1 Hva er outsourcing?

Outsourcing er også kjent som *tjenesteutsetting,* og er en stadig økende trend (Qi & Chau, 2012), spesielt i industrien (Lee, Yeung & Hong, 2011). I Norge ser man at stadig flere virksomheter velger å outsource hele eller deler av deres IKT-tjenester til tjenesteleverandører (Kommunal- og moderniseringsdepartementet, 2015). For å forstå hva outsourcing innebærer må man først kort klargjøre begrepet *sourcing.* Begrepet er en handling der virksomheter overfører arbeid, ansvar og beslutningsrettigheter til noen andre. Med hensyn til dette handler *outsourcing* om å flytte en tjeneste, aktivitet og/eller ansvar over til en ekstern part, ofte en ekstern leverandør. Dette gjøres ofte for at virksomheter kan drifte billigere, bedre, mer effektivt eller for å kunne utnytte en virksomhets ressurser optimalt (Power, Desouza & Bonifazi, 2006). En ekstern leverandør kan være både en tjenesteleverandør eller en annen. I forbindelse med studiens formål innebærer outsourcing å overføre ansvar av IKT-infrastruktur og/eller drift over til en tjenesteleverandør. Forholdet mellom operatør og tjenesteleverandør er gjerne kontraktuelt bundet gjennom en Service level Agreement (SLA), som beskriver de forventede tjenestene outsourcingen skal inneholde.

I petroleumssektoren omfatter IKT-infrastruktur og/eller drift ofte industrielle automatiserings-, kontroll- og sikkerhetssystemer, i tillegg til informasjonssystemer (DNV GL, 2015). Outsourcing av IKT-driften innebærer drift av virksomhetens nettverk, funksjoner og infrastruktur. Dette omfatter maskiner og programmer som håndterer informasjon, ofte med elementene nettverk, servere, applikasjoner, software og kabler som sammen utgjør IKT-infrastruktur (Gottschalk, 2005a; Wei & Peach, 2006). På bakgrunn av dette kan outsourcing av IKT-tjenester forstås som en bevisst beslutning om å tjenesteutsette IKT-aktiviteter, -prosesser og/eller -tjenester som er nødvendig for drift av virksomheten til en ekstern tjenesteleverandør (Majdán, 2012). Outsourcing

begrenses ikke nødvendigvis til tjenester som flyttes ut til eksterne aktører. Det kan også inkludere varer og tjenester en virksomhet kjøper fra en ekstern part, selv om de ikke har blitt produsert internt i virksomheten tidligere (Gottschalk, 2005a). Det vil si at sourcing kan forekomme internt og eksternt, hvor virksomheter velger å beholde eller sette ut hele eller deler av deres IKT-tjenester. Det velges ofte en kombinasjon av dette basert på selektive vurderinger (Gottschalk, 2005b).

Når virksomheter setter ut tjenester til ekstern leverandør omtales dette som outsourcing, uavhengig om det er innenlands eller til utlandet (Gottschalk, 2013). Utover dette er det et skille når det gjelder outsourcing, avhengig av hvor man setter ut tjenester. Dersom virksomheter velger leverandør eller partner i lavkostnadsland, som India, Kina eller Øst-Europa, omtales dette som *offshoring*. Dette er attraktivt for å redusere kostnader uten nevneverdig kvalitetsforringelse og for å tilegne ny kompetanse, samtidig som det kan gi mindre risiko og lavere investeringer (Gottschalk, 2013; Lunnan & Lervik, 2015; Solli-Sæther, 2016). Store aktører i IT-bransjen er selskaper som TCS, HCL og Wipro blant flere, der samtlige er fra India, som er et land Norge gjerne outsourcer til. Utover India er også Kina, Bangladesh, Sri Lanka, Polen, Ukraina og Litauen aktuelle land. Dersom man velger en lokal tjenesteleverandør, det vil si innenlands, omtales dette som *onshore outsourcing* (Gottschalk, 2013). I Norge er selskaper som Capgemini, Evry og Atea blant flere aktuelle leverandører, og det vises til at mange virksomheter vurderer å outsource ytterligere tjenester (Jørgenrud, 2017b). Omfanget av outsourcing i Norge er på omtrentlig 30 milliarder kroner, og markedet vokser med 10-15 prosent årlig (Nassimbeni et al., 2012; Remen & Tomter, 2017b).

2.2 Tjenester og infrastruktur

Ett av de vanligste funksjonsområdene for outsourcing er informasjonssystemer og infrastruktur, der IT-oppgaver som outsources typisk er rutineoppgaver som applikasjonsutvikling, programmering, enhetstesting og systemvedlikehold. Når det gjelder fellestjenester er det ofte systemadministrasjon, nettverksstyring, infrastruktur og brukerstøtte (Gottschalk, 2013; Wei & Peach, 2006). I Norge er det rundt 53 prosent av virksomheter som outsourcer IKT-tjenester helt eller delvis, og dette innebærer både drift og store IT-prosjekter (Næringslivets sikkerhetsråd, 2016). Eksempelvis er Statoil ett av selskapene som har satt ut vedlikehold av blant annet det tekniske nettet (Remen & Tomter, 2017b). I tillegg velger enkelte virksomheter å outsource hele

IT-funksjonen, som innebærer vedlikehold av IKT-infrastrukturen (Wei & Peach, 2006). Dette gjorde for eksempel Helse Sør-Øst, der deres moderniseringsprosjekt innebar å outsource både infrastruktur og drift (Tomter & Remen, 2017). Drift av IKT-infrastruktur er et vesentlig område for de fleste virksomheter, og digitalisering vil trolig føre til mer outsourcing i fremtiden. Spesielt gjelder dette ved bruk av skytjenester (PwC, 2017).

2.3 Informasjonssikkerhet i petroleumssektoren

Informasjonssikkerhet i petroleumssektoren, med særskilt fokus på operatører av olje- og gassplattformer, innebærer sikring av informasjon i alle virksomhetens ledd, herunder leting, feltutvikling, produksjon og transport. Informasjonssikkerhet handler om å ivareta informasjonens konfidensialitet, integritet og tilgjengelighet, som innbefatter beskyttelse mot uønskede hendelser og beskyttelse mot intenderte hendelser (Torjusen, 2013). I de senere årene har oljeplattformene gått fra å være på et lukket nett med proprietære systemer til nettbaserte systemer med internett-teknologi. Denne digitaliseringen av oljeplattformene innebærer overføringer av store mengder produksjonsdata, fjernvedlikehold- og operasjoner, i tillegg til at prosessutstyr og kontrollsystemer er avhengig av digital teknologi. Dette gjør det tilnærmet umulig å holde prosesskontrollsystemene adskilt fra informasjonssystemene og åpne nett (DNV GL, 2015; Forsvarets forskningsinstitutt, 2016). Oljebransjens produksjonssystemer og administrasjonssystemer smeltes stadig mer sammen, grunnet utviklingen mot det som omtales som integrerte operasjoner (IO). Dette er samhandling i sanntid mellom operasjonsrom, der fjernstyring av prosesser på sokkelen utføres av personell som sitter på land (Røsjø, 2009). Integrerte operasjoner medfører større krav til tilgjengelighet og integritet. For prosessanlegg og kontrollsystem innebærer det at uautoriserte personer eller systemer ikke skal kunne endre data, eller ha tilgang til systemenes funksjoner. Det skal også sørges for at autorisert tilgang ikke hindres, verken under vanlig drift eller nødprosedyrer (Torjusen, 2013). Det faktum at informasjonssystemer er vitale for alle operasjoner som utføres i forbindelse med olje- og gassvirksomhet, gjør at sektoren er digitalt sårbar i alle verdikjedenes ledd (DNV GL, 2015).

2.4 Lovverk og standarder

Et sentralt sektorregelverk er petroleumsloven (1996) med underliggende forskrifter. Regelverket stiller krav til forebyggende-, risikoreduserende- og konsekvensreduserende tiltak i sektoren, men

er ikke konkretisert og tilpasset IKT-sikkerhet (NOU 2016:19). Forebyggende IKT-sikkerhet er først og fremst virksomhetenes ansvar. Dette fremkommer av petroleumsloven § 9-3, som skal bidra til å hindre bevisste anslag mot innretninger i petroleumssektoren (DNV GL, 2015; NOU 2016:19; NUPI, 2018). Aktuelle forskrifter[1] fremhever at virksomheter skal ha styring og kontroll på informasjonssikkerhetsområdet, noe som bør være en integrert del av virksomhetens helhetlige styringssystem.

Petroleumstilsynet er sektormyndighet med overordnet ansvar for sikkerhet i bransjen. Sikkerhetsarbeidet vedrørende IKT drives imidlertid med svak styring fra myndighetene (Forsvarets forskningsinstitutt, 2016), og Ptil har ikke operativt fokus på digitale sårbarheter (DNV GL, 2015). Overvåkning, varsling og hendelseshåndtering er tjenester som tilligger aktører som NSM, NorCERT, Politiets sikkerhetstjeneste (PST) og Forsvaret, men kun dersom virksomhetene selv oppretter avtale om det (DNV GL, 2015; NOU 2016:19). Grunnet en delvis kompleks oppbygging og ansvarsfordeling når det kommer til IKT-sikkerhet (NOU 2015:13, NUPI, 2018) fremstår forebyggende IKT-sikkerhet fragmentert (DNV GL, 2015). Ingen av de selvstendige rettssubjektene i petroleumssektoren er per dags dato underlagt sikkerhetsloven. Det foregår derimot endringer i sektoren vedrørende lovverk og ansvarsfordeling med hensyn til IKT-sikkerhet, der det avventes om petroleumssektoren delvis vil inkorporeres i sikkerhetsloven (NOU 2016:19; NUPI, 2018).

Petroleumsnæringen har gjennom interesseorganisasjonen Norsk olje og gass (NOG) utarbeidet spesifikke retningslinjer for informasjonssikkerhet ved IKT-baserte prosesskontroll-, sikkerhets-, og støttesystemer. Retningslinjene er basert på ISO 27001/2-standarden (NVE, 2017). Da virksomhetene er ansvarlig for egen IKT-sikkerhet, har Ptil bedt de vurdere egen IKT-sikkerhet opp mot retningslinjene (Forsvarets forskningsinstitutt, 2016). De mest relevante i denne sammenheng er NOG 104, NOG 110 og NOG 123.

NOG 104 er obligatorisk for alle medlemmer i Norge, og inneholder 19 krav med det formål å forbedre informasjonssikkerheten i petroleumssektoren. Her stilles det krav til sikkerhetsstyring og risikoanalyser, der sistnevnte skal utføres på alle installasjoner. Videre gis det veiledning på

[1] Rammeforskriften, 2001, §10; Styringsforskriften, 1969, §4; Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) §15

hvordan man kan implementere de ulike kravene i prosessanlegg og IKT-systemer (Norsk olje og gass, 2016; Grønli, 2012). NOG 123 gir retningslinjer som er anbefalt for klassifisering av prosesskontroll og IKT-systemer basert på kritikalitet, det vil si indikatorer på viktigheten av et IKT-system basert på konsekvensene av tap og uregelmessig funksjonalitet (Norsk olje og gass, 2009b). Denne støtter blant annet ett av kravene i NOG 104, ved å gi retningslinjer for kritikalitetsvurdering (Torjusen, 2013). I tillegg gir NOG 110 retningslinjer for informasjonssikkerhet i prosesskontroll og IKT-systemer (Norsk olje og gass, 2009A).

Det er gjennomført et felles industriprosjekt lansert av DNV GL, der resultatet er en retningslinje for beste praksis vedrørende hvordan olje- og gassoperatører kan håndtere cybertrusler (Torp, 2017). Videre er det en standard for informasjonssikkerhet når det gjelder prosessanlegg i petroleumssektoren (Torjusen, 2013). Denne heter IEC/ISA 62443, sikkerhet for industriell automasjon og kontrollsystem, og beskriver elementene som inngår i et system for cybersikkerhet, og hvordan man kan møte de ulike kravene (ISA, u.å.).

2.5 Fordeler og risikoer knyttet til outsourcing

I et miljø preget av økt konkurranse og omstilling må virksomheter kontinuerlig fokusere på ressurser og kjernevirksomheter, for å holde seg konkurransedyktig og operere mer effektivt. Som en følge av dette har outsourcing av IKT-tjenester blitt stadig mer omfattende (Fan et al., 2012), både i omfang og former (Qi & Chau, 2012). Som nevnt står petroleumssektoren overfor et behov for omstilling og effektivisering, mye grunnet et paradigmeskifte og digitalisering i bransjen (Røsjø, 2009).

Når det gjelder motivatorer for outsourcing kan man skille mellom teknologiske, organisatoriske, politiske, taktiske og strategiske perspektiver (Liang et al., 2016), der de to sistnevnte er mest utbredt. Tradisjonelt sett har outsourcing i stor grad blitt betraktet å handle om reduserte kostnader ved å sette ut IKT-tjenester som ikke er kjerneaktiviteter, som samtidig gir økt fokus og tid på virksomhetens primære formål (Fell, 2013; Oshri et al, 2011). Eksempelvis reduseres kostnadene med outsourcing til lavkostnadsland ved en tredjedel (Niazi et al., 2013). På en annen side handler en strategisk tilnærming om hvordan virksomheter kan dra fordeler ved å benytte seg av IKT-markedet, der tilgang til ferdigheter og ekspertise anses som ledende årsaker til at virksomheter velger å tjenesteutsette IKT-tjenester (Fell, 2013). I tillegg kan det bidra til høyere effektivitet og

produktivitet, reduksjon og kontroll på driftskostnader, samt tilgang på kompetanse, ressurser og kunnskap (Frost, 2000; Power et al., 2006; Gottschalk, 2005a). I dag betraktes outsourcing stort sett som en strategisk beslutning (Power et al., 2006), som følge av en holdningsendring og økt konkurransepress. Det er nødvendig at virksomheter omstiller seg for mer effektive forretningsprosesser og optimaliserer ressursbruken, i tillegg til at ledere presses for å øke ytelse, resultatvekst og aksjonærverdi (Frost, 2000).

Til tross de mange fordelene outsourcing kan bidra til, innebærer det også utfordringer og risikoer som kan lede til uønskede konsekvenser (Fan et al., 2012). Outsourcing er en krevende prosess, grunnet mange og komplekse risikofaktorer knyttet til tekniske, organisatoriske, finansielle og juridiske forhold (Dhillon et al., 2017; Goodman & Ramer, 2007; Prado, 2011). Argumenter mot outsourcing er ofte risikoen knyttet til avhengigheten mellom forretningsprosess og IT-tjenester, dog går det langt ut over dette (van Scheers, 2016). Det fører blant annet til en forlenget og avhengig forsyningskjede, der enhver feil kan føre til forstyrrelse i forsyningnettverket (Lee et al., 2011). Outsourcing øker bekymringer rettet mot sikkerhet og etterlevelse av eksterne og interne krav (Bachlechner, Thalmann & Maier, 2013), økonomisk stilling og omdømme, samt tap av kontroll og autonomi (Prado, 2011). Spesielt kritisk er risikoen når det gjelder konfidensialitet og uautorisert tilgang til private og sensitive data, som kan kompromittere en virksomhet og dens suksess (Frost, 2000; Prado, 2011). Risikoer ved outsourcing av IKT-tjenester er imidlertid langt fler, der det i følgende tabell er utarbeidet en oversikt av risikoer med relevans for studien.

Risiko	Spesielle bekymringer
Compliance	- Sikkerhet - Etterlevelse av krav - Konfidensialitet - Tap av informasjon
Strategisk	- Manglende ekspertise - Ikke forventet tjenestelevering - Regulative/juridiske vansker - Manglende sikring hos leverandør - Kulturelle og språklige forskjeller
Operasjonell	- Teknisk feil - Tap av kontroll og autonomi - Svindel og/eller feil - Uautorisert tilgang til systemer og informasjon - Tilsiktede handlinger
Organisatorisk	- Økte kostnader - Omdømme - Tap av kunnskap og kompetanse - Tillit - Sikkerhetspolicy
Teknisk	- Internettsikkerhet - Nettverk - Reguleringer

Tabell 1. Risikoer ved outsourcing, egendefinert. *(Basert på Bachlechner et al., 2013; Dhillon et al., 2017; Prado, 2011; van Scheers, 2016).*

Outsourcing er en vanskelig prosess grunnet de mange og komplekse risikofaktorer (Dhillon et al., 2017; Goodman & Ramer, 2007; Prado, 2011), og mange virksomheter mislykkes i prosessene (Liu et al., 2010; Qi & Chau, 2012). Risikoen vil påvirke hvorvidt virksomheter beslutter å outsource eller ikke, der enkelte virksomheter har betydelig risikovillighet mens andre i større grad har risikoaversjon (Gottschalk, 2005a). Det hevdes dog at enkelte suksessfaktorer vil ha en direkte effekt på utfallet når det gjelder outsourcing, og er det som skiller suksess fra fiasko. Suksessfaktorer defineres som kunnskap om egen kjernevirksomhet og ressurser, kunnskap om egenskaper ved IT-systemene og tilhørende behov, optimalisering av tjenestetilgang og systemintegrasjon, valg av strategi og prioriteringer, samt kriterier av valg av leverandør med fler (Gottschalk, 2005b).

2.6 Uønskede hendelser

Det har inntruffet mange uønskede hendelser som følge av outsourcing av IKT. Hendelsene som ble nevnt innledningsvis handler om virksomheter som har valgt å outsource tjenester til lavkostnadsland, som har resulterte i uheldige situasjoner. Fellestrekket hos flere er at uautorisert personell har hatt tilgang til systemene og/eller sensitiv data. Som følge av dette har konsekvensene for flere vært økonomisk store, og personer har måtte tre av stillingene sine. Dette har også ført til kritikk rundt sikkerheten til samtlige (Hotvedt & Røset, 2017; Remen & Tomter, 2017a; Remen & Tomter, 2017b; Tomter & Remen, 2017).

Helse Sør-Øst outsourcet IKT-infrastrukturen og drift i 2016, med det mål å få en digital oppgradering og redusere kostnader. Det ble avdekket at flere IT-arbeidere i Asia og Øst-Europa hadde hatt tilgang til sensitiv pasientinformasjon, og mulighet for å hente ut pasientdata til over 2,8 millioner mennesker. Dette førte til en intern gransking med bistand fra PricewaterhouseCoopers (PwC), og granskning fra Datatilsynet (Tomter & Remen, 2017). PwC konkluderte med at Helse Sør-Øst ikke hadde tilstrekkelig IKT-sikkerhet, der manglende kontroll på tilgangsstyring, manglende risikovurderinger og utilstrekkelig vurdering av risikoer ved informasjonssikkerhet ble fremhevet (PwC, 2017). Datatilsynet ga kraftig kritikk for manglende risikovurderinger, og ila helseforetakene 800 000 kr hver i bot - til sammen 7.2 millioner (Tomter & Remen, 2017).

I 2017 ble det avdekket at svenske myndigheter hadde outsourcet IKT-tjenester til utenlandske aktører, som hadde hatt tilgang til svært sensitiv informasjon. Det fremkom at Transporttilsynets registre og identitet til hemmelige agenter kunne ha kommet på avveie, der sensitiv informasjon var tilgjengelig for tsjekkiske IT-arbeidere uten nødvendig sikkerhetsklarering. I tillegg skal de ha hatt tilgang til informasjon om infrastrukturen som bruer, veier og havner, som kan utgjøre en høy risiko dersom noen ønsker å skadeliggjøre dette (Hotvedt & Røset, 2017).

Nødnettet driftes av Motorola og Broadnet, der sistnevnte outsourcet IT-drift til det indiske selskapet Tech Machindra. Ved en tilfeldighet ble det oppdaget at en IT-arbeider i India hadde gjennomført uautorisert pålogging til Nødnettet for å gjøre vedlikeholdsarbeid. Dette er kritisk, da Nødnettet skal driftes fra Norge, da det er underlagt sikkerhetsloven, og arbeidere med tilgang må ha autorisering. Tilgangen IT-arbeiderne hadde innebar mulighet til å stenge ned Nødnettet, og

kunne medført alvorlige konsekvenser (Remen & Tomter, 2017a). Gransking av saken viste flere brudd på sikkerhetsloven og Ekom-loven, i tillegg til manglende risikovurderinger og sikkerhetsforståelse når det kommer til outsourcing hos flere av de involverte aktørene (Remen, Tomter & Flaarønning, 2017).

Statoil outsourcet både kontor- og teknisk nett til HCL i 2014. En konsekvens av dette var da raffineriet på Mongstad stoppet, som følge av at en indisk IT-arbeider gikk inn på en server han ikke skulle hatt tilgang til. Dette er kun én av flere hendelser som har inntruffet som følge av at IT-arbeidere i India har brutt barrierer på plattformer, landanlegg og sentralt i Statoil. Hendelsen på Mongstad skjedde under en blandingsprosess, som førte til at bensin rant ut i vannet og forurenset. Den økonomiske kostnaden ble på litt under en million kroner. Det indiske selskapet hadde også ansvar for drift og vedlikehold av Statoils tekniske nett, noe som førte til uautoriserte påloggingerr til flere plattformer. Situasjoner som evakuering, manglende data og nedetid for nettverket er flere hendelser som Statoil har opplevd de siste årene (Remen & Tomter, 2017b).

Maersk ble rammet av et virus sommeren 2016, som hele konsernet globalt ble påvirket av. Viruset kom seg først inn i ytre sone, og klarte derfra å komme seg dypere inn og påvirke samtlige kontorer, noe som førte til nedetid på store deler av kontorene til Maersk (Fribo, 2017). Det ble i etterkant påpekt at det er behov for en forbedring i infrastrukturen (Chirgwin, 2018), og at det ble benyttet kjent angrepsmetode (Jørgenrud, 2017a). Dette kan indikere et manglende fokus og kontroll på samtidens risikoer. Virksomheten har tidligere blitt kritisert for IKT-sikkerheten, noe dette angrepet underbygger (Fribo, 2017).

Hendelsene belyser utfordringer som kan oppstå som følge av outsourcing, der samtlige hendelser bortsett fra Maersk hadde utfordringer med uautorisert personell inne i systemene. For Maersk kan dette knyttes til sårbar infrastruktur på de ulike kontorene deres, som bidro til at viruset klarte å komme inn i systemene. De ulike hendelsene viser en bredde i sårbarhetene knyttet til digitale utfordringer, der manglende kontroll og risikovurderinger er et fellestrekk hos flere. Det er på bakgrunn av dette interessant å undersøke hvordan risikovurderinger vedrørende outsourcing av IKT-tjenester benyttes for å kartlegge risiko knyttet til tjenesteutsetting, og hvilke forhold som spiller inn på eksperters vurdering.

3. Teori

I følgende kapittel vil studiens teoretiske rammeverk presenteres. Da studien søker å se hvordan risikovurderinger benyttes i tilknytning til outsourcing er det viktig å legge til grunn teori om risikostyring. Dette inkluderer elementer som risikovurdering, risiko og sårbarhet, i tillegg til faktorer som kan påvirke risikovurderinger. Da risikovurderinger kan påvirkes av hvem som gjennomfører dem er risikopersepsjon inkludert. Det er i tillegg vektlagt hvorfor operatører velger outsourcing, og det er i den sammenheng valgt å legge til grunn beslutningsteori som et resultat av risikovurdering. Risikostyring reflekterer den overordnede prosessen som skal sikre etterlevelse ved outsourcing, der risikovurdering er et verktøy som skal hjelpe med dette. Følgelig avdekkes risiko og sårbarhet gjennom risikovurderinger, og det er viktig å være bevisst på disse skillene.

3.1 Risikostyring

Risikostyring er helheten av prosesser, funksjoner, styring, aktører og regler, der handlinger og mål bestemmes på bakgrunn av relevant risikobilde. Det innebærer hvordan man styrer, kommuniserer og håndterer beslutninger (Aven & Renn, 2012), inklusivt metoder, prosesser og strategier som benyttes for å kunne avdekke og vurdere risiko (Aven, 2015a). Outsourcing av IKT-tjenester fører til økt kompleksitet og avhengighet som følge av forlenget verdikjede, der dette kan resultere i uønskede hendelser og konsekvenser (Fan et al., 2012; Nassimbeni et al., 2012; Niazi et al., 2013). I den forbindelse er det bekymring knyttet til styring og håndtering av risiko (Prado, 2011; Willcocks & Lacity, 1999). For å ivareta gode prosesser og beslutninger ved outsourcing er god risikostyring en forutsetning. En god prosess vil også ha effekt på hvorvidt man lykkes med å sette ut en tjeneste (Aris et al., 2008). Da risikostyring er en overordnet prosess, er det i studien inkludert interne og eksterne faktorer som er viktige i en risikostyringsprosess. Faktorene skal bidra med å danne en helhet av operatørenes valg i forbindelse med outsourcing. De kan bidra med innsikt og forståelse for hva som vektlegges i den totale vurderingen, samtidig som det konkretiserer og viser hva som er av betydning.

Noe av det viktigste ved outsourcing er å vurdere risiko (Prado, 2011). Risikostyring er en utfordrende prosess, der problemer ofte oppstår grunnet manglende forståelse og innsikt i grunnleggende aspekter. Dette gjelder en forståelse for hva risiko er, samt hvordan man beskriver og kommuniserer risiko. I tillegg er problemer knyttet til hvordan man benytter analyser, samt

vurderer akseptabel og ikke-akseptabel risiko (Aven, 2007). Eksempelvis gjenspeiles flere av disse aspektene i outsourcingen til Helse Sør-Øst (PwC, 2017). Hvordan operatører gjennomfører risikostyring i forbindelse med informasjonssikkerhet kan ha direkte innvirkning på IKT-sikkerheten. I tillegg foregår risikostyring både på virksomhets- og sektornivå, og er følgelig aktuelt når man undersøker hvordan eksperter forstår og vektlegger risikoelementer i forbindelse med outsourcing. Således utgjør dette rammen for studien, og spesielt ettersom operatørers risikostyring legger føringer for ekspertenes vurderinger av risiko.

Gode kontraktuelle forpliktelser og relasjonell styring i forbindelse med outsourcing av IKT-tjenester er vesentlig for prosessen (Loukis & Kyriakou, 2018). Mange virksomheter mislykkes med outsourcing grunnet manglende kompetanse og implementering av risikostyring, selv om bevisstheten rundt prosessen er høy (Aris et al., 2008). Nye tendenser antyder at risikovurdering, håndtering og kommunikasjon ikke er tilstrekkelig til å analysere og forbedre risikostyringsprosesser, for eksempel i forbindelse med outsourcing av IKT-tjenester. Karakteristikkene av moderne komplekse og gjensidige avhengige risikoer krever nye konsepter som er i stand til å håndtere (beskrevne) utfordringer (Aven og Renn, 2012).

For at virksomheter skal kunne lykkes med outsourcing er robust risikostyring en kritisk suksessfaktor, der man identifiserer, anerkjenner og håndterer risiko (Aris et al., 2008; Prado, 2011; Samantra et al., 2013). Således handler det om å utforske muligheter for å skape verdier samtidig som man søker å unngå tap (Aven, 2010). Mangler i startfasen eller manglende risikostyring kan øke sannsynligheten for negative konsekvenser for en virksomhet. I forbindelse med outsourcing må risikostyring være en iterativ prosess, med høy bevissthet grunnet stadig nye trusler og risikoer (Aris et al., 2008; Prado, 2011). Det må gjennomføres en rekke handlinger og aktiviteter, der formålet er å få innsikt i alle forhold og hendelser som kan påvirke en virksomhet. Risikostyring skal bidra til å vurdere strategiske alternativer og risikovillighet (Aven, 2010; Aven, 2015a), og inkluderer blant annet risikovurdering og beslutningstaking (Aris, et al., 2008; Prado, 2011).

3.1.1 Rammebetingelser

Rammebetingelser er relevante forhold når det kommer til styring av risiko (Aven, Boyesen, Njå, Olsen & Sandve, 2004), spesielt da karakteristikker i omgivelsene kan ha innvirkning på

risikovurderinger ved outsourcing (Prado, 2011). Kontroll med risiko omfatter et bredt spekter av mekanismer, som går fra egenkontroll til myndighetsregulering (Engen et al., 2016). Rammebetingelser utgjør en indirekte påvirkning ved at de spiller inn på blant annet handlingsrom og samhandlingsmuligheter. Det er gjerne forhold aktører ikke har kontroll over, og er ofte forårsaket av tidligere beslutninger i egen eller annen virksomhet, eller på et annet organisatorisk nivå (SINTEF, 2009). Individer påvirkes av faktorer i omgivelsene (Rasmussen, 1997), og det må derfor hensyntas når man skal forstå eksperters vurderinger. Noe som er gjennomgående kritisk er at beslutningstakeres vurdering avhenger av aktiviteter fra andre, der det ofte er press fra ulike fagmiljøer. Dette kan føre til at man mister kontroll over det totale risikobilde og skape målkonflikter, som kan påvirke muligheten for sikker håndtering (Rasmussen, 1997; SINTEF, 2009). I risikovurderinger må man dermed ta hensyn til alle forhold som kan ha innvirkning på vurderingene, samtidig som konteksten til ekspertene bør reflekteres.

3.1.2 Risiko og sårbarhet

Risiko handler om fremtidige hendelser, som potensielt kan ha negative og positive utfall for noe en virksomhet verdsetter (Njå, Solberg & Braut, 2017). I forbindelse med outsourcing kan dette handle om risiko knyttet til blant annet tekniske, organisatoriske, finansielle og juridiske forhold (Dhillon et al., 2017; Goodman & Ramer, 2007; Prado, 2011). I denne sammenheng søkes det å se på hvordan eksperter forstår risikoen med å outsource sine IKT-tjenester og/eller drift. Når det gjelder IKT-systemer og risikoer relatert til informasjonssikkerhet kan dette være vanskelig å klassifisere. Bakgrunnen er at det er stor usikkerhet knyttet til mulige konsekvenser. For å håndtere dette kan risikoanalyser og verdivurderinger gi nødvendig innsikt. Samtidig kan det være hensiktsmessig å vurdere forsiktighetsstrategier for å hindre overraskelser (Aven et al., 2004).

Når det gjelder outsourcing er også sårbarhet et velkjent fenomen, som er en feil eller egenskap i et system som en trusselaktør kan utnytte. Dette kan føre til uautorisert tilgang til organisatoriske verdier (Landoll, 2006). Moderne informasjonssystemer inneholder millioner av programkoder som kontrollerer kritiske funksjoner gjennom flere avhengige og distribuerte systemer, sensorer og operasjoner. Disse komplekse systemene illustrerer utfordringen med å forstå de dynamiske integrerte systemene, som består av mennesker, prosesser og teknologier (Akhgar & Hamid, 2014). Sårbarheter i IKT-systemer eller verdikjeder kan være en trussel mot organisatoriske verdier (Feng, Wang & Li, 2014), og det er derfor viktig å kartlegge og vurdere dem for å

identifisere restrisiko (Landoll, 2006). Det er behov for et sett med vurderingskriterier, slik at man kan beskytte kritiske verdier (Feng et al., 2014). Gjennom risikostyringsprosessen bør virksomheter utlede vurderingskriterier og akseptabel risiko, noe som kan styrke eksperters evne til å vurdere restrisiko knyttet til outsourcing. I tillegg bør risikovurderinger inkludere blant annet kritikaliteten til informasjonen, samt konsekvensen av tap av konfidensialitet, integritet og tilgjengelighet (Goodman & Ramer, 2007).

3.2 Risikovurdering

For å undersøke hvordan risikovurderinger benyttes av eksperter ved outsourcing er det hensiktsmessig å belyse hvordan risikovurderinger avhenger av hvem som vurderer og hva som vurderes (Aven et al., 2004). Med andre ord vil det være av betydning hvordan eksperter forstår risiko i konteksten vedrørende outsourcing.

Risikovurdering er en prosess der formålet er å beskrive og vurdere risiko som kan føre til negative konsekvenser (Aven, 2015b). Dette bør være et integrert element i en virksomhets risikostyring, med det formål å danne et godt beslutningsgrunnlag (Aris et al., 2008; Prado, 2011). Risikovurderinger har betydning for både det styrende, gjennomførende og kontrollerende informasjonssikkerhetsarbeidet (Direktoratet for e-helse, 2016). Målet er å støtte beslutningstaking ved å generere kunnskap om risiko og tilhørende konsekvenser i en gitt kontekst (Aven & Guikema, 2011; Renn, 2008). Når det gjelder risiko som truer sikkerhetsmålene til informasjonssikkerhet, herunder *konfidensialitet, integritet* og *tilgjengelighet,* er det viktig å være bevisst på at omfanget av risikofaktorer er stort. I forbindelse med outsourcing av IKT er ofte risikofaktorene gjensidig avhengige av hverandre, og derfor er det nødvendig å se på sammenhengende faktorer så vel som uavhengige (Fan et al., 2012). Risikovurderinger må søke å avdekke alle områder som kan påvirke informasjonssikkerheten, der håndtering av sikkerhetsmålene er av størst bekymring (Dhillon et al., 2017). Klassiske risikovurderinger består av tre elementer; risikoidentifisering, risikoanalyse- og evaluering:

- Risikoidentifikasjon handler om å avdekke risikofaktorer knyttet til outsourcing (Fan et al., 2012; Prado, 2011).

- Risikoanalyse innebærer å estimere og beskrive risiko (Prado, 2011). Hensikten er å samle inn nødvendig informasjon, med det formål å vurdere problemstillinger og risikoer som kan oppstå dersom man velger å outsource en tjeneste (Aris et al., 2008).
- Risikoevaluering er dermed prosessen der man evaluerer resultatene fra risikoanalysen (Aven, Røed & Wiencke, 2008).

Risiko i forbindelse med informasjonssikkerhet er kompleks og avhengig av flere elementer, samt at det står over mange utfordringer. Økte kostnader ved sikkerhetsbrudd, økt omfang av sofistikert dataangrep, komplekse omgivelser og krav om etterlevelse av regelverk viser til noen dimensjoner som er fremtredende (Cezar, Cavusoglu, & Raghunathan, 2014). Med andre ord, risiko knyttet til informasjonssikkerhet gjenspeiles ikke bare av egen praksis, men avhenger av andres sikkerhetsmekanismer i tillegg (Wu et al., 2017). Risiko påvirkes dermed både av enkeltpersoners, virksomheters og sektorens praksis rundt informasjonssikkerhet. Uønskede hendelser i forbindelse med outsourcing av IKT-tjenester kan innebære både intenderte og ikke-intenderte hendelser. Det vil si at utfordringene er mange, der flere samfunnsnivå kan ha innvirkning på det totale risikobildet.

Risikovurderinger skal bidra til gode beslutningsprosesser. For å sikre dette, og dra nytte av fordelene som outsourcing medfører, er det avgjørende at risikoer avdekkes og håndteres (Tafti, 2005). Det er totaliteten av elementene analyse og evaluering som sammen utgjør en risikovurdering (Aven, 2007), men planlegging er også et viktig element (Rausand & Utne, 2009). I evalueringsfasen er det viktig med kommunikasjon og konsultasjon til involverte aktører, for å sikre at de forstår hva som vektlegges og hvordan de ulike aspektene balanseres mot hverandre (Aven og Renn, 2012). Det er dermed en mulighet for å inkludere enkeltpersoner i ulike virksomheter og/eller myndighetsnivå, for å drøfte resultatene før man tar en endelig beslutning vedrørende outsourcing.

3.2.1 Klassiske risikovurderinger og black swans

Bruk av klassiske risikovurderinger er ikke alltid tilstrekkelige da omfanget av mulige utfall og/eller tilhørende sannsynlighetene ofte er utydelige (Renn, 2007). Spesielt gjelder dette ved hendelser omtalt som 'black swans', der dette forstås som en overraskende ekstrem hendelse i forhold til kunnskapen man har (Aven, 2015c). På bakgrunn av dette må man alltid ta høyde for

hvem som vurderer hendelsen, tidsaspektet og konteksten (Aven, 2014). I forbindelse med risikovurderinger vedrørende informasjonssikkerhet er det ikke mulig å identifisere alle relevante risikoer i en gitt situasjon, og man må være bevisst på at det også vil være uoppdagede trusler. Dette er et mønster som er gjentakende ved informasjonssikkerhet, der problemer oppstår uventet og plutselig (Oppliger, 2015). Kunnskap og usikkerhet er vesentlige momenter for å kunne imøtekomme risikoer som black swans representerer, fordi risikovurderinger inkluderer kunnskap, data og informasjon som er basert på ekspertenes forståelse (Aven, 2015c). Når det kommer til denne typen risiko argumenteres det for at det er nødvendig med nye metoder for å kunne håndtere slike hendelser (Aven, 2015c; Oppliger, 2015).

Ved hendelser som er vanskelige å forutse, eller som kommer overraskende, kan det være effektivt med en robust tilnærming (Aven, 2014). Det er fordi man ikke har tilstrekkelig informasjon til å beregne sannsynlighet for at en hendelse inntreffer og forventet konsekvens på en fornuftig måte (Oppliger, 2015). Det bør derfor benyttes forsiktighetsprinsipper. Dette gjelder eksempelvis bruk av sikkerhetsbarrierer, fleksibelt design, forbedre ytelse av barrierer, redundans og vedlikehold, samt søke å være en resilient virksomhet. Sistnevnte innebærer at man forbereder seg på forstyrrelser, variasjon og endring (Aven, 2014). Fremtredende trusler ved outsourcing er eksempelvis hackerangrep og spionasje, som vil si ukjente risikoer. På bakgrunn av dette er det ikke nødvendigvis tilstrekkelig med klassiske risikovurderinger, og er elementer som bør tas i betraktning når man evaluerer resultatene.

3.2.2 Risikopersepsjon

Risikovurderinger blir påvirket av hvilke holdninger, erfaringer, verdier og egenskaper man har, samt eksterne forhold eller parter (Engen et al., 2016). Viktige forskjeller eksisterer blant ulike deltakere og interessenter, der aktørene kan ha ulik persepsjon når det gjelder risiko tilknyttet outsourcing (Liu et al., 2010). Spesielt kan dette være i petroleumssektoren, der ansvarsdelingen er fragmentert og det ikke er tydelige lovverk som legger klare føringer. Risikovurderinger er subjektive, og representerer en blanding av psykologiske, sosiale, kulturelle og politiske faktorer (Slovic, 2001). Det er viktig å være tydelig på at ulike aktører vektlegger risikofaktorer forskjellig, og dermed også viktigheten av faktorene (Liu et al., 2010). Det er formålstjenlig å undersøke hvordan eksperters persepsjon påvirker deres risikovurderinger, og følgelig hva de vektlegger.

Det er ofte en sammenheng mellom risikofaktorer som avdekkes, der disse blir evaluert basert på subjektivitet fra de ulike deltakerne (Fan et al., 2012). Vurderingene bør inkludere kunnskap fra flere funksjonelle områder i en virksomhet, noe som krever samarbeid og laginnsats (Fell, 2013). Spesielt gjelder dette for outsourcing av IKT-tjenester da det er risikofaktorer knyttet til ulike fagområder (Tafti, 2005). Det er viktig å være bevisst på at ulike interessenter trolig har ulik oppfattelse av risiko. Identifisering av risikofaktorer i IKT-prosjekter har gjerne vært begrenset til en interessentgruppe, for eksempel prosjektledere (Qi, Wu, Zhang & Li, 2012). Risikopersepsjonen kan påvirke hvilke beslutninger operatører tar vedrørende outsourcing, og kan bidra til en helhetsforståelse av konteksten og de beslutninger som tas.

3.3 Beslutningstaking

I dette kapittelet er det lagt frem hvordan risikovurderinger skal danne grunnlag for velinformerte beslutninger når det gjelder outsourcing av IKT-tjenester. Beslutningstaking er vanskelig, spesielt i situasjoner med høy risiko og stor usikkerhet, og det er vanskelig å forutsi konsekvensene av beslutninger som tas (Aven, 2007). Inkludering av beslutningstaking i denne sammenhengen bidrar til forståelse av de valg og vurderinger som operatørene har tatt vedrørende outsourcing.

Risikovurderinger innebærer at man vurderer ulike løsninger og alternativer som kan imøtekomme mål og krav fastsatt av interessenter (Aven, 2007). Beslutninger om outsourcing innebærer to valg; først om man skal outsource, og deretter hvilken modell man skal velge (Gottschalk, 2013). Ofte foreligger beslutningskriterier, prinsipper eller standarder som gir føringer når man vurderer risikoen, og som kan forenkle beslutningsprosessen (Aven et al., 2004). Underlaget man har gjennom blant annet risikovurderinger vil sjeldent være tilstrekkelig i form av å inneha begrensninger. Det er utfordrende å få med alle aspekter av betydning for en virksomhet, og vekten beslutningstaker tillegger vurderingene kan være avhengig av ulike faktorer (Aven, 2007). Enkelte eksperter vil være offensive i henhold til risiko og usikkerhet, med en større aksept for risiko dersom verdien i aktiviteten kan være stor (Aven, 2015a). Beslutning om outsourcing av IKT-tjenester er et strategisk valg, der det er viktig at ledere fra alle funksjonsområder deltar i beslutningsprosessen (van Scheers, 2006). En avgjørende faktor ved risikovurderinger og beslutningstaking kan dermed være ens holdning til usikkerhet. I den forbindelse er en strategi å anvende en forsiktighetstilnærming.

3.3.1 Forsiktighetsprinsippet

Forsiktighetsprinsippet innebærer at man skal vise varsomhet dersom risikoen er usikker. Dette betyr at man skal unngå å starte en aktivitet dersom risikoen er usikker, eller implementere risikoreduserende tiltak dersom dette kan redusere risikoen (Aven og Renn, 2012). Prinsippet har økt i bruk de senere årene, som delvis skyldes globalisering, der risiko strekker seg over tid og landegrenser (Lofstedt, 2003). Ved outsourcing av IKT-tjenester øker sårbarhetene proporsjonalt med verdikjeden. I tillegg øker antallet risikoer og eksponeringer etter hvert som nettverk, system, lovverk og politiske føringer knyttes sammen til et stort antall aktører (Goodman & Ramer, 2007). Kompleksiteten med ukjente risikoer og mulige alvorlige konsekvenser kan indikerer et behov for forsiktighet. Dette gjelder spesielt ved beslutninger som baseres på risikovurderinger vedrørende outsourcing.

Gjennom outsourcing introduseres informasjonssikkerhet for nye risikoer ved at det åpnes opp for flere eksponeringsmuligheter, angrep eller ulykker (Goodman & Ramer, 2007). Økt verdikjede innebærer økt eksponering, og følgelig et økt behov for forsiktighet når man skal vurdere risikoene knyttet til outsourcing. Imidlertid argumenteres det for at forsiktighetsprinsippet er 'a state of mind', heller enn en beslutningsregel, som bidrar til at man blir mer sensitiv over usikkerhet, tvetydighet og uvitenhet (Renn, 2007). Dette kan påvirke risikovurderingene, og legge føringer for hvordan risikovurderinger og beslutninger gjennomføres. Således handler ivaretakelse av informasjonssikkerheten ved outsourcing å være bevisst på flere aspekter.

3.4 Læring

Læring er en prosess der mennesker og virksomheter tilegner seg ny kunnskap, og på bakgrunn av det endrer sin atferd. For at virksomheter skal lære er det en forutsetning med kunnskapsdeling innad (Jacobsen & Thorsvik, 2007), noe som er et av hovedaspektene med risikovurderinger. Risikovurderinger bidrar til kollektiv læring, der kompetansen som oppnås deles og samles med det mål å nyttiggjøres i virksomheten (Dalin, 1999). Læring og styring innad i virksomheter, mellom virksomheter, og mellom virksomheter og eksterne aktører er forhold som kan påvirker eksperters vurdering av risiko. Det er derfor nødvendig å inkludere læring for å forstå dens betydning i relasjon til beslutninger om outsourcing.

Erfaringer oppnås både ved vanlige og uvanlige hendelser, der sjeldne hendelser kan være positivt for læring (Engen et al., 2016). Hendelser som er sjeldne gir virksomheter et innblikk i deres forutsetninger for å håndtere det uforutsette, og legger dermed grunnlag for forbedring (Lampel, Shamsie & Shapira, 2009). Ettersom hendelser av denne karakteren belyser styrker og svakheter (Kim, Kim & Miner, 2009), er dette et område som er viktig når man skal forstå vurderinger og beslutninger med tanke på outsourcing. Det er flere uønskede hendelser som har kommet frem der outsourcing har vært en viktig del av det totale bildet. Ved inkludering av læring mellom personer, virksomheter og eksterne aktører vil det danne en forståelse for hvordan dette er medvirkende i eksperters vurdering og beslutning vedrørende outsourcing.

3.4.1 Organisatorisk kontekst

Enhver virksomhet befinner seg i et miljø som defineres av relevante elementer i omgivelsene, og anses dermed som den eksterne konteksten. I så måte innebærer organisatorisk læring den eksterne kontekst, der elementer blant annet er kultur, teknologi, mål og strategi (Betten & Pettersen, 2015). For å forstå andre virksomheters påvirkning, samt sektorens betydning generelt sett, er det viktig å belyse hvordan den organisatoriske konteksten kan være en medvirkende årsak vedrørende beslutninger om outsourcing. I slike grenseoverganger mellom virksomheter og eksterne instanser ligger det et potensial for læring som møtes i ulike praksisfellesskap. Man beveger seg her utover sitt avgrensede område og knytter kontakt med andre, der man overfører kunnskap og informasjon som bidrar til felles utvikling (Wenger, 1998). Muligheten for å benytte seg av tilgjengelige aktiviteter, andre deltakere, relasjoner, ressurser og informasjon er et sentralt aspekt ved læring på denne arenaen (Kvale & Nielsen, 1999). Dermed handler det om en helhetlig tilnærming for størst mulig læringsutbytte, der ulike grenseobjekter, som tilsyn og direktorat, utgjør arena for samhandling, læring og kunnskapsdeling (SINTEF, 2011). Inkludering av læring innad i sektoren vil følgelig gi bedre helhetlig forståelse for eksperters risikovurdering og beslutninger i relasjon til outsourcing.

4. Metode

I følgende kapittel vil det redegjøres for studiens valg av forskningsstrategi og metodiske tilnærming, samt begrunnelse for de valg og vurderinger som er tatt underveis. Problemstillingen har lagt føringer for fremgangsmåten som har blitt benyttet.

4.1 Studiens hensikt, valg av teori og forskningsstrategi

Da studien har som formål å undersøke hvordan operatører vurderer og vektlegger risiko når det gjelder outsourcing av IKT-tjenester, er det valgt å benytte en abduktiv forskningsstrategi. Strategien er hensiktsmessig når det undersøkes hvordan aktører oppfatter fenomener i deres kontekst (Blaikie, 2010) herunder hvordan eksperter tolker risiko i deres omgivelser. Den er i tillegg formålstjenlig når det benyttes etablert teori som utgangspunkt for studien, for å forstå fenomenet som forskes på (Thagaard, 2013). Det er i den sammenheng benyttet teori om risikostyring, risikovurdering, beslutningstaking og læring. Fokuset i studien er hvordan eksperter, herunder personer i operatørselskap som jobber med informasjonssikkerhet og/eller IT, forstår og vurderer risiko knyttet til outsourcing. For å inkorporere ulike aspekter som kan påvirke ekspertenes vurderinger og forståelse av risiko, er det undersøkt interne og eksterne faktorer på virksomhetsnivå, i tillegg til læring og styring i sektoren. Til sammen utgjør dette en helhetsvurdering av ulike momenter som kan ha påvirkning for eksperters vurdering og persepsjon av outsourcing. Således danner det fundament for å forstå hvordan dette utgjør beslutningsgrunnlag. Strategien er benyttet for å kunne tolke, forstå og belyse outsourcing, som anses hensiktsmessig når man skal belyse fenomenet i dets sosiale kontekst (Danermark, 1997).

4.2 Casestudie

Dette er en eksplorativ casestudie fordi den belyser et komplekst fenomen der flere variabler er av betydning, samt hvordan prosesser har foregått over tid (Yin, 2014). I lys av at petroleumssektoren digitaliseres, er det fremhevet et manglende fokus på informasjonssikkerhet (IRIS, 2018; Røsjø, 2009). På bakgrunn av dette har det vært en søken etter å belyse outsourcing av IKT hos operatører, der risiko og sårbarhet er en sentral del. Det har blitt inkludert flere operatører innen petroleumssektoren, der kunnskap fra forskjellige har blitt innhentet og utviklet. Dermed har dette vært en studie av utforskende art, som har vært nyttig for å etablere en forståelse av et komplekst og utfordrende samtidsfenomen der paralleller til andre sektorer kan trekkes. Casestudie kombinert

med en abduktiv forskningsstrategi har vært hensiktsmessig i den empiriske fremstillingen, der resultatene har blitt vurdert sammen som en helhet for å undersøke kausale forklaringer (Yin, 2014).

4.3 Metodisk tilnærming

Det er benyttet en kvalitativ tilnærming (Blaikie, 2010), ettersom det har vært en søken etter hvordan aktører forstår og vurderer risiko i forbindelse med outsourcing av IKT-tjenester. Tilnærmingen har vært formålstjenlig da den har bidratt til dybdeforståelse og nyanser når det gjelder eksperters risikovurderinger og risikoforståelse. Tabell 2 presenterer studiens prosess og utgangspunktet for å beskrive valg og veien mot mål.

Når	Forventet utbytte	Faktisk utbytte
Des -17	Finne tema og problemstilling. Utarbeide prosjektskisse. Planlegge startfase.	Tema og problemstilling. Utarbeidet prosjektskisse. Planla startfasen.
Jan-18	Innledende arbeid Utarbeide utkast til innledning, kontekst og teori. Planlegge empirisk innsamling. Kontakte aktuelle operatørselskap og informanter.	Innledende arbeid godt i gang, bortsett fra kontekst. Utarbeidet metodekapittel. Kontaktet aktuelle operatørselskap.
Feb-18	Videreføre arbeidet med kapittel 1-3. Utarbeide metodekapittel. Planlegg datainnsamling, herunder utforming av intervjuguide og avtale med informanter	Utarbeidet intervjuguide. Avtalt med informanter. Gjennomført fem intervjuer. Fullført kap. 1-4, samt utkast av kapittel 5.
Mar-18	Empirisk innsamling. Transkribering og analyse av materialet. Utarbeide første utkast av empirisk kapittel.	Gjennomført fire intervjuer. Innhente og analysere dokumenter. Utarbeidet utkast av kapittel 5.
Apr-18	Utarbeide empiri og diskusjonskapittel. Raffinering av teori.	Gjennomføring av 1 intervju Ferdigstille kapittel 1-7.
Mai-18	Videreføre empiri og diskusjonskapittel Utarbeide konklusjon Ferdigstille kapittel 1-7	Ferdigstille hele oppgaven. Levere til informanter for gjennomgang. Endelig innlevering!
Jun-18	Ferdigstille	-

Tabell 2. Tidsplan.

Arbeidet med studien startet i desember -17, som følge av de mange outsourcinghendelsene som har vært i media. Da IKT-sikkerhet er et felt i utvikling, innebærer det således mange problemstillinger som må belyses. Dette gjør følgelig studien svært dagsaktuell, også i tiden fremover.

4.3.1 Datakilder

Det ble gjennomført datatriangulering (Blaikie, 2010) da det er benyttet data fra fagdokumenter, forskningslitteratur og semi-strukturerte intervjuer. Hensikten med å kombinere datakilder var å sikre tilstrekkelig kunnskap om, og innsikt i, risiko og risikovurderinger i forbindelse med outsourcing. Innhenting av eksisterende kunnskap ga større forståelse for outsourcing allerede fra startfasen, og la føringer for analysen. Innsamling av data kan også bidra til å se det teoretiske rammeverket på nye måter (Yin, 2014), og teorien har dermed blitt raffinert underveis. Det ble valgt en kombinasjon mellom intervju av relevante eksperter i sektoren, og fagdokumenter som fokuserer på informasjonssikkerhet og digitale trusler. For å få et godt situasjonsbilde av outsourcing og ekspertenes risikovurdering i tilknytning til tjenesteutsetting av IKT-tjenester, ble det i intervjuene lagt opp til diskusjon av både fagdokumenter og forskningslitteratur som har blitt benyttet.

Utvalg av dokumenter

I startfasen av studien ble det innhentet og gjennomgått forskning om outsourcing, med fokus på risiko og risikostyring. Eksisterende forskningslitteratur utgjorde således et viktig grunnlag, og ga føringer for aktuelle problemstillinger og datainnsamling. I tillegg dannet det et rammeverk for analysen. Et selektivt utvalg er redegjort for i delkapittel 1.3.

Dokumenter utgjør relevant datakilde (Yin, 2014), og det er derfor innhentet fagdokumenter som inneholdt informasjon med vesentlige elementer knyttet direkte til ett eller flere av forskningsspørsmålene. Hensikten er å etablere et godt datagrunnlag (Grønmo, 2004), og har gitt en utfyllende og nyansert forståelse av outsourcing, risiko og utfordringer knyttet til dette. Fagdokumentene som benyttes er utarbeidet av blant annet Norges sikkerhetsmyndighet (NSM), som er Norges nasjonale fagmiljø innenfor IKT-sikkerhet. De belyser deriblant informasjonssikkerhet og outsourcing fra et faglig perspektiv. Videre er det innhentet rapport fra Norwegian Institute of International Affairs (NUPI), som har intervjuet virksomheter i

petroleumssektoren om digitale trusler, sårbarheter, reguleringer og ansvar. Det er også innhentet rapport fra International Research Institute of Stavanger (IRIS), som belyser digitalisering i petroleumssektoren. Fagdokumentene er både sektorspesifikke når det kommer til IKT-sikkerhet relatert til petroleumssektoren, samt at de belyser outsourcing fra et faglig ståsted som kan benyttes uavhengig av sektor. Da problemstillingen bærer preg av både sektorspesifikke og sektoruavhengige elementer anses det hensiktsmessig å legge til grunn fagdokumenter som ivaretar det samme spekteret. På bakgrunn av dette har følgende dokumenter blitt benyttet:

- *NUPI (2018) «Cyber-weapons in International Politics Possible sabotage against the Norwegian petroleum sector»*
- *IRIS (2018) «Digitalisering i petroleumsnæringen»*
- *NSM (2017) «Helhetlig risikobilde 2017»*
- *NSM (2017) «Risiko 2017»*
- *NOU 2015:13 (2015) «Digital sårbarhet - sikkert samfunn»*

Utvalg av informanter

Det er flere kriterier som legger føringer for et strategisk utvalg av informanter (Johannessen, Christoffersen & Tufte, 2011), der studiens formål og avgrensing har vært medvirkende. På bakgrunn av dette har det vært en søken etter informanter som arbeider innen IKT i operatørselskap på norsk sokkel. Det er valgt å inkludere både operatører som outsourcer, og operatører som holder IKT-tjenester internt. Dette kan bidra til å undersøke likheter og forskjeller i eksperters vurderinger. Da studien søker hvilke forhold som vektlegges, vil en inkludering av begge parter gi rom for å undersøke hvilke vurderinger som er gjort. Dette inkluderer forståelsen av risiko og sårbarhet hos de ulike ekspertene, samt hvorvidt interne og/eller eksterne faktor og sektorinvolvering har vært av betydning.

Ut fra Oljedirektoratet sin liste[2] over aktive operatører på norsk sokkel, ble det sendt ut forespørsel med tilhørende informasjon om studien på e-post til 27 operatører. Da responsen i første omgang var noe lav, ble informanter kontaktet over telefon. Dette munnet ut i deltakelse fra ni eksperter

[2] Oljedirektoratet, faktasider. http://factpages.npd.no/factpages/Default.aspx?culture=nb-no&nav1=company&nav2=Attributes

fra ulike operatørselskap, som betraktes å være et representativt utvalg. Informantene har ulik kompetanse og bakgrunn, fra teknologer til økonomer. Inngangsporten har forholdsvis vært å intervjue eksperter som har vært deltakende i risikovurderinger, eller som kjenner godt til prosessene i de tilfellene risikovurderinger gjøres globalt. Tabell 3 er en oversikt over informanter, samt deres rolle i operatørselskapene. Ett av studiens forskningsspørsmål innebærer å undersøke om sektorens læring, styring og samhandling har vært av betydning i de risikovurderinger som er gjort. På bakgrunn av dette ble Petroleumstilsynet kontaktet og intervjuet.

Informant	Rolle	Outsourcer
Informant A	IS Manager	Ja, offshoring
Informant B	IT Governance team leader	Ja, onshoring
Informant C	Manager IT	Nei
Informant D	(Group) IT Manager	Nei
Informant E	IT Manager	Ja, onshore og internt
Informant F	IT Manager	Ja, onshore
Informant G	VP Data & Information management	Ja, onshore, offshore og internt
Informant H	Control and Automation Engineer	Ja, onshore
Informant I	Senior Advisor Corporate Risk	Ja, offshore og internt
Informant J	Sjefingeniør	N/A (Ptil)

Tabell 3. Oversikt over informanter.

Det ble gjennomført semi-strukturerte intervjuer med en varighet på 30-60 minutter, i perioden 15. februar til 09. april. I forkant ble det utarbeidet en intervjuguide (Se vedlegg 1 og 2), der tidligere forskningslitteratur og fagdokumenter la utgangspunkt for utforming. Hvert intervju startet med en redegjørelse om studiens hensikt, samt forespørsel om å ta intervjuet opp på bånd for å sikre informasjonen som ble gitt, noe alle samtykket til.

4.4 Analyse

Datainnsamling ble etterfulgt av dataanalyse (Blaikie, 2010), med den hensikt å redusere og analysere informasjonen som var innsamlet og i tillegg skape et rammeverk for å kunne formidle innholdet på en forsvarlig måte (Johannessen et al., 2011). I denne studien ble eksisterende dokumenter og data fra intervjuene analysert hver for seg, før rådataen har blitt satt opp mot hverandre og sett som en helhet, for å få en forståelse og tolkning av materialet.

Som en del av analyseprosessen ble alle intervjuene transkribert, senest innen en uke etter intervjuene var gjennomført. Da det er hensiktsmessig å benytte åpen- og aksial koding (Blaikie, 2010; Grønmo, 2004), ble dataen brutt ned og analysert i kategorier og underkategorier som resulterte i en oversikt. Informasjonen ble så systematisert, og plassert i en matrise etter forskningsspørsmålene. Dette fremhevet de enkeltes informantenes svar innen ulike områder, som ga mulighet til å se deres svar og fortellinger opp mot en annen. Det ble her vurdert både mønstre, likhetstrekk og ulikheter, sett opp mot kontekster, handlinger og andre kausale forhold.

Dokumentene som er innhentet ble gjennomlest i startfasen av studien, og har således lagt føringer for relevante områder og tematikker. I etterkant av intervjuene ble dokumentene gjennomgått på ny, og relevant informasjon hentet ut for å redusere datamengden. Dette grunnet at innholdet i fagdokumentene er av det omfang hvor kun elementer var relevant for studien. I tillegg kan det bidra til økt forståelse for fenomenet og problemstillingen (Grønmo, 2004). Det har vært en dynamisk prosess, og tanker om innholdet har blitt notert underveis. Dokumentene har blitt gjennomgått flere ganger, og ved å ta et avbrekk og vende tilbake til arbeidet etter tid har det bidratt til et reflektert syn på innholdet og sammenhengen. På denne måten er det også søkt å unngå tunnelsyn (Grønmo, 2004).

4.5 Reliabilitet og validitet

I forskning er det nødvendig å kvalitetssikre studien, der forskningsdesignet som er presentert utgjør et sett av logiske utsagn som kan vurderes ut fra logiske tester. To sentrale begreper er i den forbindelse reliabilitet og validitet (Thagaard, 2013; Yin, 2014).

4.5.1 Reliabilitet

Det er flere faktorer som kan påvirke studiens pålitelighet (Kvale & Brinkmann, 2009), der det er forsøkt å være bevisst på dette for å unngå skjevheter underveis i prosessen. For å styrke reliabiliteten har det vært fokus på å gi detaljert beskrivelse av forskningsprosessen og refleksjoner rundt egen fremgangsmåte (Silvermann, 2011). Dette øker bevisstheten og refleksjonen omkring egen prosess, som er viktig da egne meninger og holdninger kan være en påvirkningsfaktor med hensyn til teoribidrag og tolkninger i analysen. Videre er en av svakhetene med kvalitativ metode et mindre antall informanter, noe som kan ha betydning for hvorvidt resultatene kan bekreftes og reproduseres (Kvale & Brinkmann, 2009). Dette er spesielt fordi menneskets erindringer ikke er statiske, og deres forklaringer og erfaringer kan endres over tid, noe som kan skape utfordringer ved en senere anledning. Informantene har også ulik bakgrunn og kompetanse som kan være av betydning for resultatene som fremkommer, i likhet med kulturelle og strategiske forhold i operatørselskapet. Derimot belyser studien forhold som tidligere er trukket fram av andre instanser, noe som forsterker påliteligheten på flere områder. Dette vil ytterligere redegjøres for i diskusjonskapittelet.

4.5.2 Validitet

Validitet er knyttet til tolkning av data, og omhandler i hvilken grad det kan trekkes gyldige slutninger fra funnene (Thagaard, 2013). Gyldighet er viktig å sikre gjennom hele prosessen, der det kan skilles mellom intern og ekstern validitet (Yin, 2014).

Intern validitet

Problemstillingen har lagt føringer for datainnsamlingen. Da det undersøkes hvordan operatører i petroleumssektoren vurderer outsourcing, har innsamlingen inkludert informanter som har deltatt og/eller har kjennskap til de vurderinger som er gjort internt i operatørselskapene. I tillegg er det benyttet fagdokumenter som belyser vesentlige elementer knyttet til problemstillingen. Dette er blant annet knyttet til outsourcing i ulike sektorer, da det er argumentert for at outsourcing fører med utfordringer som er tverrsektorielle. I tillegg belyser flere fagdokumenter risiko og sårbarhet knyttet til IKT-tjenester, som studien har fokus på. Intervjuguiden har hatt utgangspunkt i forskningsspørsmålene som overordnede tematikker, for å sikre relevans og operasjonalisering. Underordnede spørsmål er utarbeidet på bakgrunn av den kunnskapen forskningslitteratur og fagdokumenter har gitt, for å sikre at vesentlige områder ble inkludert. Således øker også

validiteten (Grønmo, 2004). Gjennom prosessen har det vært fokus på å se datamaterialet opp mot problemstillingen for å ikke falle utenfor «den røde tråden», da datamaterialet har vært omfattende. Dette har også vært hensiktsmessig for å sikre relevans i henhold til studien.

Ekstern validitet

I denne studien har det blitt argumentert for at outsourcing og tilhørende utfordringer er et tverrsektorielt problem. Det kan ikke direkte avvises at det kan trekkes paralleller til lignende kontekster i andre sektorer og/eller i fremtidige situasjoner, og det er således generaliserbart (Andersen, 2006; Kvale & Brinkmann, 2009). Gjennom å gi fyldige kontekstbeskrivelser i dette og følgende kapittel, er det søkt å bidra til et grunnlag som validiteten kan vurderes ut fra, og således kan det sikres ekstern validitet (Yin, 2014). Da resultatene inkluderer empiri om dagens situasjon fra operatører, samt dokumenter som belyser elementer ved outsourcing og risiko ved IKT, uavhengig av sektor, ses flere likhetstrekk som forsterker dette. I den sammenheng kan overførbarheten sannsynliggjøres, om ikke direkte bevises (Johannessen et al., 2011).

5. Empiri

Følgende kapittel presenterer studiens empiriske funn som er innhentet gjennom fagdokumenter og intervjuer, og er strukturert etter forskningsspørsmålene. Første forskningsspørsmål belyser hvordan eksperter i operatørselskap forstår og vurderer risiko knyttet til outsourcing, som videre danner et fundament for videre oppbyggingen av studien. De neste to forskningsspørsmålene har hovedvekt på henholdsvis virksomhets- og sektornivå, og belyser interne og eksterne faktorer som kan ha innvirkning på ekspertenes vurdering. Hensikten er å inkludere operatørenes omgivelser, der ulike samfunnsnivå som andre virksomheter, tilsyn og myndigheter trekkes inn.

5.1 Hvordan forstår eksperter risiko og sårbarhet knyttet til outsourcing, og hvordan vektlegges dette i risikovurderinger?

Gjennom studien fremkommer flere forhold som er av betydning når det gjelder eksperters forståelse av risiko og sårbarhet knyttet til outsourcing av IKT-tjenester. Blant annet trekkes det frem økonomi, omdømme, språk og kultur, samt tilgang og kontroll. Hvordan ulike eksperter forstår risikoen knyttet til forholdene som belyses, og hvordan de vektlegges, er ikke nødvendigvis sammenfallende. Det søkes derfor å belyse hvorfor og hvordan dette er av betydning når vurderinger om outsourcing gjennomføres. Følgende delkapittel struktureres etter organisatoriske, kulturelle og tekniske forhold.

5.1.1 Organisatoriske forhold

Kostnad

Outsourcing av IKT-tjenester er ofte attraktivt ved at det kan gi kostnadsfordeler for en virksomhet (NOU 2015:13; NSM, 2018; Kommunal- og moderniseringsdepartementet, 2015). Derimot er det flere av informantene som påpeker at kostnad er en risiko, spesielt sett mot outsourcing til lavkostnadsland. Det trekkes paralleller til at outsourcing kan føre til leveranse av dårligere tjenester og tjenester som kan falle utenfor avtalen. Dette kan blant annet medføre skjulte kostnader: *«Du ser på papiret at denne outsourcingen blir billig og det blir fint. Så er det ett eller annet som faller litt utenom [...] Det som faller utenom må du ta selv eller få andre til å ta. Og det koster jo penger»* [Informant B]. I tillegg nevner flere informanter at backsourcing og stor turnover i lavkostnadsland kan føre til en økt risiko, der eventuell lav kostnad ikke er verdt risikoen som outsourcing medfører.

Redusert kvalitet på tjenestene er noe som vektlegges i vurderingene. Dette benyttes gjerne som et argument for å holde tjenestene internt, eller for å velge leverandør i Norge. Her benevner to informanter at de ikke opplever det spesielt dyrere å velge lokal leverandør, i den forstand at de kan tilby konkurransedyktige betingelser og god kvalitet på tjenestene. Dette gir indikasjoner på at kostnad ikke er av stor betydning når det skal velges tjenesteleverandør. Imidlertid belyser fagdokumenter at outsourcing kan gi mer stabile og tilgjengelige tjenester (NOU 2015:13; NSM, 2017a; NSM, 2018), som også kan ha en innvirkning på den totale kostnaden.

Verdier

Tjenesteutsetting gir forhøyet risiko når det gjelder informasjonssikkerhet, som følge av komplekse og uoversiktlige verdikjeder. For å kunne beskytte verdiene er det av vesentlig betydning at man er klar over risikoene som outsourcing åpner opp for. Det stilles derfor høye krav til virksomheter når det gjelder kontroll over hvilke verdier de har, samt hvordan og hvorfor disse må sikres dersom man velger å outsource (NSM, 2017a; NSM, 2017b; NSM, 2018). Imidlertid er det ingen informanter som nevner konfidensialitet, integritet og/eller tilgjengelighet i forbindelse med sine vurderinger. Dette er interessant fordi god IKT-sikkerhet krever bevissthet rundt sikkerhetsmålene, i tillegg til grundige verdivurderinger (NSM, 2018). Øvrig er det stor variasjon i hva informantene betrakter som kritisk informasjon i deres virksomhet, der det tolkes dit hen at de har forskjellig forståelse av verdien på informasjonen de besitter. Informantenes ulike bakgrunn og kultur i operatørselskapene kan påvirke risikoforståelsen knyttet til informasjonsverdier, der det også kan påpekes at informasjonssikkerhet er et relativt nytt fagområde for petroleumssektoren. Det er på bakgrunn av dette nødvendig med en endret tilnærming til informasjonssikkerhet hos operatørene, da det er tidligere belyst at utfordringene som kommer krever ny system- og situasjonsforståelse (IRIS, 2018).

Tre av informantene mener informasjonen de har er virksomhetskritisk, og har dermed et stort fokus på å opprettholde god informasjonssikkerhet gjennom blant annet standarder og interne krav. Informant C presiserer dette ved å si at «*vi er mer strengere og religiøs enn paven føler jeg*». Samtidig er det kun det operatørselskapet som har valgt å holde tjenestene sine internt som følge av risikoen outsourcing har for tap av informasjon. Av de resterende informantene vurderer fire av dem informasjonen og data etter kritikalitet, ved å gjennomføre verdi- og/eller

konsekvensvurderinger. Det kan nevnes at de operatørselskapene også outsourcer hele IKT-infrastrukturen, inkludert drift. Her påpeker én informant viktigheten av å skape bevissthet rundt informasjonen man har, og forteller at det er viktig at direktører på ulike nivå forstår verdien av dataen de eier. Ved å ha eierskap til informasjonen aksepterer de potensielle konsekvenser dersom de beslutter å outsource. Manglende kontroll og eierskap over egen data er tidligere pekt på som en risiko ved outsourcing, der kunnskap om dette bidrar til risikoreduksjon og bevissthet (NSM, 2017a; NSM, 2017b; NSM, 2018). En annen fremhever at mindre kritisk data er lettere å sette ut. Begge utsagn kan antyde at informantene enten ikke vurderer informasjonen som kritisk og/eller at de mener de har gode sikringstiltak. Én informant, i et operatørselskap som ikke outsourcer, presiserer at informasjonen de har er av betydning for virksomheten, men karakteriserer den likevel «*ikke som rikets sikkerhet*» [Informant D]. Dermed ville konsekvenser av hendelser kun vært av betydning for operatøren selv. Overnevnte viser indikasjoner på svært forskjellig forståelse for og eierskap til verdiene hos informantene. Dette virker å skille seg fra andre sektorer som behandler informasjon og opplysninger som er hjemlet i lov, eksempelvis kraft eller helse.

Omdømme

Hele verdikjeden til petroleumsvirksomheter er i økende grad utsatt for digitale trusler og sårbarheter, som kan forsterkes av outsourcing. Uønskede hendelser kan føre til informasjon på avveie, og dermed ha konsekvenser for blant annet styringsevne, økonomi og omdømme (NOU 2015:13; NSM, 2018). Tre av informantene vurderer omdømme som den største risikoen ved å outsource, og vektlegger dette mest i deres vurderinger. Dette er de samme informantene som ser på operatørens informasjon og data som kritisk, og som arbeider svært aktivt med å utarbeide standarder og interne krav for informasjonssikkerhetsarbeidet. Omdømme var ett av hovedkriteriene i vurderingene til operatørene, der to likevel har valgt å outsource IKT-tjenestene.

Oppsummering av organisatoriske forhold

Når det gjelder organisatoriske forhold anses omdømme å være den største risikoen ved outsourcing, og får følgelig høyest prioritering i risikovurderingene. Flere av ekspertene vektlegger videre kvalitet på tjenestene, fordi dårlige tjenester kan medføre flere negative konsekvenser. Generelt sett er det variasjon hos ekspertene vedrørende risikoforholdene som er gjennomgått, der de også vektlegges forskjellig. Mest kritisk fremstår likevel mangel på eierskap og bevissthet med tanke på informasjon og verdier. Spesielt fordi manglende forståelse for nødvendigheten av å sikre

informasjonen enklere kan medføre beslutning om å tjenesteutsette IKT-tjenester, basert på dårlige og/eller feilaktige vilkår.

5.1.2 Kulturelle forhold

Flertallet av informantene fremhever kulturelle forhold som en risiko med å sette ut tjenester til lavkostnadsland. Kulturelle forhold er i denne sammenheng språk og kommunikasjon, kultur og forståelse, samt brukervennlighet. Dette er interessant da slike utfordringer ikke fremkommer i fagdokumenter. Det er flere informanter som påpeker hvordan brukervennligheten har innvirkning på den totale risikoen ved outsourcing.

Det er gjentagende hvordan informantene ser på språkforskjeller som en utfordring, og fremhever at «*det er jo en ganske vesentlig sikkerhetsrisiko, det med språkbarrierer, forståelse, kultur og alt dette som ikke er så veldig lett å liksom bare ta i en matrise»* [Informant G]. Det kommer frem at språk blant annet er rot til misforståelser, og flere har negativ erfaring fra samarbeid med tjenesteleverandør grunnet dette. Flere informanter forteller at de tidvis har måtte ty til nødløsninger som kommunikasjon via chat fremfor telefon, noe som kan være kritisk dersom det haster. Kommunikasjonen kan også påvirkes av andre faktorer, som tidssone og avstand, noe som skaper relasjonelle utfordringer som påvirker samarbeidet. For operatørene utgjør dette elementer som ikke nødvendigvis inngår i en kontraktsinngåelse, og beskrives som tidkrevende og belastende. Dermed påvirker det brukervennligheten, og indikerer således å være en risiko som er av direkte betydning for enkelte operatørers valg når det kommer til outsourcing og/eller tjenesteleverandør.

Kultur trekkes også frem som et vesentlig risikomoment hos informantene, noe som kan medføre utfordringer ved den daglige driften. Spesielt fremheves kultur hos tjenesteleverandører i lavkostnadsland, der *«[...] det aldri er noen problemer. Og de vil jo aldri finne på å si eller spørre hvor de ikke forstår, eller om det er smart det du foreslår. Det vil de aldri si, på grunn av kulturen.*» [Informant C]. Flere informanter fremhever i den forbindelse at det er problematisk å jobbe effektivt sammen med tjenesteleverandører i andre kulturer. Det er flere som har dårlige erfaringer med tjenesteleverandører i lavkostland, som har ført til et ønske om tjenesteleverandører lokalisert nærmere Norge. Flere av informantene som har valgt å sette ut IKT-tjenester til Norge forteller å ha valgt det på bakgrunn av en forståelse for bransjen og tilhørende prosesser.

Flere informanter fremhever lojalitet som en utfordring, uavhengig av om det er innenlands eller lavkostnadsland. Alle informantene, bortsett fra én, peker på at lojalitet er til selskapet man jobber i. Det vil si hos tjenesteleverandøren, og kan således være en risiko. I den sammenheng reflekterer én informant over at eventuell outsourcing ville ført til konstant skepsis til tjenesteleverandør, der de måtte ha brukt mye tid på å følge dem opp. I tilknytning til kultur uttrykker to informanter også bekymring for arbeidsforholdene, og den innvirkningen dette kan ha på kvaliteten i arbeidet og følgelig på sikkerheten. Språk og kultur virker å være av betydning for flere informanter i forbindelse med outsourcing, der kriterier er satt mot lokalisering av tjenesteleverandør og bransjeforståelse. Det ses at dette vektlegges mest av operatørene som har valgt leverandør innenfor landets grenser, og det påpekes også at kulturen har vesentlig innvirkning på kvaliteten på tjenestene. Flere av informantene som vektla kulturelle forhold nevner at sikkerheten vil forbedres ved valg av leverandør innenlands med bransjeforståelse fremfor tjenesteleverandør i lavkostnadsland.

Oppsummering av kulturelle forhold

Kulturelle forhold fremstår som et viktig moment i eksperters risikovurdering, og har innvirkning på både risiko, økonomi og samarbeid. Samtlige eksperter reflekterer over kulturelle forskjeller, og de som har erfaring med outsourcing til lavkostland har lite positivt å fortelle. På ulike måter vektlegges kulturelle forskjeller i eksperters vurdering når det gjelder outsourcing, og generelt får det høy prioritering. Dette begrunnes med kvalitet, brukervennlighet og effektivitet. Kulturelle forhold er et område der ekspertene er enige om den økte risikoen som outsourcing til lavkostland medfører, der ingen ville valgt dette selv.

5.1.3 Tekniske forhold

En generell risiko som forsterkes når man setter ut IKT-tjenester utenfor Norge er redusert kontroll på tekniske sikringstiltak og tilgang til data. Dette forsterkes etterhvert som verdikjedene øker i kompleksitet, samtidig som det fører til redusert kontroll hos en virksomhet (NOU 2015:13; NSM, 2017a; NSM, 2017b; NSM, 2018). Det er varierende blant informantene hvorvidt de er villig til å outsource IKT-tjenester, der vurderingene hos enkelte handler om påvirkningen en eventuell hendelse kan ha. Det skilles mellom produksjonsnett og kontornett, der det varierer hvilke tjenester som er satt ut.

Tekniske tiltak varierer fra mikrosegmentering av både produksjonsnettet og kontornettet, til mindre sikkerhetstiltak rundt kontornettet hos andre. Informant A forteller at «*det som er litt av utfordringen er at det er større og større behov for integrasjon mellom produksjonsnettene, riggnettene og dette her*». Dette krever bedre sikkerhet på hele den digitale plattformen, noe som kan være utfordrende fordi det fører til et komplekst grensesnitt. Flere vektlegger IKT-sikkerhet som en prosess, der det er fokus på å ha barrierer og forsinke dersom noen skulle klare å trenge inn i systemene. Sikkerhetstiltakene som er innført hos operatørene eksemplifiserer hvordan informantene forholder seg til IKT-sikkerhet, noe som antyder forskjellig forståelse i bransjen. At det fremkommer et fokus på tekniske forhold og barrierer kan ses i lys av informantenes kompetanse og sektorspesifikke barrieretenkning, der flere har bakgrunn med teknisk kompetanse.

Kontroll

Kontroll over IKT-systemer og -infrastruktur er ett av risikoområdene som utpeker seg i forbindelse med outsourcing, grunnet forlenget og kompleks verdikjede som det er vanskelig å ha oversikt over (NSM, 2017a; NSM, 2017b). En tredjedel av informantene mener at å sette ut tjenester øker risikoen, der én trekker frem at det «*er flere fiender der ute enn det var før*» [Informant C]. Fagdokumenter indikerer større bekymring med tanke på angrep mot leverandører, i tillegg til at det fokuseres på økt trussel gjennom innsidere (NSM, 2017a; NSM, 2017b; NUPI, 2018; PST, 2017). Et interessant moment er at ingen av informantene trekker sistnevnte fram som en risiko. Som nevnt er det derimot flere informanter som peker på lojalitet til egen virksomhet. Slikt sett fremstår lojalitetsaspektet hos informantene noe naivt sett mot den økte trusselen. Spesielt fordi IKT-systemer er sårbare overfor innsidere, der de blant annet kan utnytte en legitim tilgang til systemet til uautorisert formål (NSM, 2017a; NUPI, 2018).

Én informant fremhever risikoen med manglende kontroll over tjenesteleverandør, ved å fortelle at *«du vet ingenting hva de gjør miljøet ditt. Da måtte jeg jo brukt vanvittig mye tid med å følge opp det»* [Informant D]. Manglende kontroll er en av årsakene til at operatøren har holdt tjenestene sine internt, da oppfølging av tjenesteleverandør ville vært en utfordring. Dette nevnes av flere andre informanter, men vektlegges ikke i deres vurderinger. Imidlertid er det slik at tjenesteutsetting ikke innebærer at virksomhetens ansvar reduseres eller forenkles. Derimot vil det føre med seg betydelig større ansvar når det kommer til kontroll av tjenesteleverandør, inkludert å sikre informasjonsverdier (NSM, 2017b).

Operatørene som outsourcer til Norge gjennomfører regelmessige audits på tjenesteleverandørene for å ha kontroll. Derimot er det svært interessant at operatører som outsourcer utenfor Norge ikke oppgir å følge opp tjenesteleverandører på samme måte. For at virksomheter skal kunne redusere risikoen med tjenesteutsetting fordrer det et robust kontrollregime (Justis- og beredskapsdepartementet, 2016a). Det bemerkes at ingen av informantene som outsourcer, uavhengig av lokasjon på tjenesteleverandør, anser sitt oppfølgingsansvar som en risiko.

Tilgangsstyring

Det er sårbarheter forbundet med tjenesteutsetting, der spesielt tilgang til data er et risikomoment. Tilgangsstyring er et viktig sikringstiltak for å hindre at personer ikke har større tilgang enn det som er tjenstlig behov. Dette reduserer også muligheten for å utnytte tilgangen de enkelte har til systemene (NSM, 2017a). Flertallet av informantene trekker frem tilgang til data og systemer som en risiko med å outsource IKT-tjenester, der de uttrykker behov for kontroll over hvem som har tilgang til deres data. En informant forteller at de holder «*brukertilgang på et minimum på alle kontoer som må ha tilgang til systemet*» [Informant E]. Dog oppleves det at enkelte av operatørene som outsourcer tar lett på oppgaven og overlater kontroll til tjenesteleverandør. Det er kun én av informantene som påpeker eget ansvar vedrørende kontroll over tilganger. Når det gjelder operatørene som ikke outsourcer virker det som de har et konservativt tilgangsstyringsregime, som beskrives ved at «*det må være need to have, not nice to have*» [Informant C]. Selv om det er fokus på tilgang, og det benevnes som en risiko, er det få som forteller om konkrete sikkerhetstiltak for å redusere risikoen. Det er kun én som vektlegger lokal kontroll, som er vesentlig i deres vurderinger, der de i tillegg ønsker mer teknisk kompetanse on-site.

Tilgangsstyring er et virksomhetsansvar, der det handler om å øke robustheten ved å lukke sårbarheter knyttet til virksomhetens IKT-systemer (NSM, 2017a). Etterlevelse av tilgangsstyring kan være en utfordring, der sikkerhetsmålene tilgjengelighet og konfidensialitet er motstridende. Tilgjengelighet handler om å ha nødvendig tilgang ved behov, mens konfidensialitet innebærer at informasjonen ikke blir kjent for uvedkommende (NOU 2015:13). Selv om soneinndeling og teknisk segmentering av nettverk er gode sikkerhetstiltak for å begrense tilgang, kreves det leverandørtilgang inn til enkelte funksjoner som utgjør sårbarheter i den totale verdikjeden (NUPI, 2018). Det er en utfordring for virksomheter å ha full oversikt og kontroll, spesielt grunnet økt avhengighet mellom operatører og leverandør. Dette fører til at det kreves bedre oppfølging av

underleverandører, der en grunnleggende forutsetning er risikovurderinger. Videre må man risikovurdere innsyn i virksomhetens informasjon og systemer, samt tilgangsstyring (NSM, 2017a; NUPI, 2018). Ingen av informantene har risikovurdert egen drift for å kartlegge behov eller nødvendig sikkerhetsnivå. Behovet for risikovurderinger øker når IKT-tjenester driftes utenfor landets grenser, grunnet forsterket risiko når det gjelder tilgang (NSM, 2017a; NUPI, 2018). Tross de påpekte risikoer ved tekniske forhold, er det få av informantene som prioriterte dette i vurderingene, bortsett fra informanten som også vektla lokal kontroll.

Vedlikehold

Et annet risikoaspekt ved outsourcing er vedlikehold av systemer og programvare, samt forebygging av sårbarheter. Mangelfullt vedlikehold kan skape unødvendige sårbarheter og føre til at menneskelige sårbarheter utnyttes, eksempelvis manglende sikkerhetsoppdateringer (NOU 2015:13; NSM, 2017a). Sårbarheter i systemer er en risiko hos flertallet av informantene, der de rutinemessig gjennomfører penetrasjonstester. Dette innebærer forsøk på å trenge seg inn i infrastrukturen, noe som kan bidra til å forbedre sikkerhetstilstanden. Dog viser det seg at tekniske tiltak, eksempelvis sikkerhetspatching, ofte ikke utnyttes tilstrekkelig (NOU 2015:13; NSM, 2017a; NSM, 2017b). Derimot kreves det mer enn tekniske tiltak for å kunne sikre systemene (NSM; 2017b), da en ensidig tilnærming ikke gir effektiv beskyttelsesmekanisme. Informantene har ikke fokus rettet mot hvordan gamle systemer er sårbare for uønskede hendelser, og dermed fremkommer det ikke av betydning i vurderingene.

Oppsummering av tekniske forhold

Når det kommer til tekniske sikkerhetstiltak er det stor variasjon i hvilke tiltak operatørene implementerer. Det er også bemerkelsesverdig at bestilleransvaret, herunder oppfølging og revisjoner av tjenesteleverandør, ikke tydeligere vektlegges som en risiko ved tjenesteutsetting. Operatører som outsourcer innad i Norge forteller om audits og revisjoner av tjenesteleverandør, mens det er fraværende hos de som benytter tjenesteleverandør utenfor landets grenser. Uavhengig av dette anser ingen av ekspertene, bortsett fra én, sitt oppfølgingsansvar som en risiko. Det er heller ingen som har risikovurdert egen drift i forkant av beslutninger om outsourcing, og dermed fremkommer det ikke i vurderingene deres.

5.2 I hvilken grad har interne og eksterne faktorer betydning for operatørers vurderinger vedrørende outsourcing?

Flere faktorer fremstår å være av betydning i operatørenes vurderinger, som både er av intern og ekstern karakter. Interne faktorer kan knyttes opp mot kostnad og tilgang til ekspertise som er vesentlig for virksomheters drift. Eksterne faktorer finnes derimot i omgivelsene, og kan ha påvirkning på valg og vurderinger vedrørende outsourcing. Disse faktorene kan være en medvirkende årsak til hvordan eksperter vurderer risiko, som kan påvirke vurderingene både bevisst og ubevisst. Ved å inkludere interne og eksterne faktorer som kan være av betydning for eksperters risikovurderinger blir grunnlaget for å forstå beslutningene mer solid.

5.2.1 Interne faktorer

Kostnad og fokus på kjerneaktivitet

Virksomheter tar ofte en strategisk beslutning ved å sette ut IKT-tjenester. Motivasjonen er gjerne redusert og stabile kostnader. Dette gjelder spesielt fjerndrift fra lavkostnadsland (NOU 2015:13; NSM, 2017a; NSM, 2018; Kommunal- og moderniseringsdepartementet, 2015). Tidligere ble det trukket fram hvordan kostnad betraktes som en risiko, hvorav det kun er to informanter som nevner pris som et insentiv ved å outsource. Begge arbeider i operatørselskaper som har satt ut tjenester helt eller delvis til lavkostnadsland. De samme informantene trekker i den sammenheng frem at outsourcing ikke var et alternativ, hvor én forteller at *«når det gjelder generelt sett outsourcing av IT-drift så er dette en opplagt sak for oss, at vi ikke skal være et IT-driftsselskap»* [Informant G]. For dem bidrar outsourcing til økt fokus på kjernevirksomheten, og kan føre til økonomisk gevinst for operatøren totalt sett, da de i større grad kan konsentrere seg om virksomhetsmål.

Outsourcing kan føre til at arbeidsdagen forenkles, da det redusere arbeidsbelastningen (IRIS, 2018). Hos informantene er dette synet noe motstridene; noen mener oppfølgingsansvaret blir mye jobb, mens andre mener outsourcing vil lette arbeidsdagen. Én informant forteller at «*stresset tas ut av hverdagen*» [Informant F]. Begge sidene viser seg å ha innvirkning på den totale vurderingen, og virker å utgjøre en underliggende faktor hos enkelte som har valgt outsourcing.

Tilgang på ekspertise og kompetanse

Når man outsourcer tjenester kan det gi tilgang til stabile fagmiljøer og spisskompetanse innen IKT. Ofte er slike fagmiljø mer robust når det gjelder kompetanse enn det virksomheter har mulighet til å opprettholde selv over tid. Dog er virksomhetene samtidig avhengig av å opprettholde et minimum selv, der en risiko ved tjenesteutsetting er at virksomheter mister kompetanse (NSM, 2017a; NOU 2015:13). Halvparten av informantene fremhever at tilgang til kompetanse innen forskjellige fagområder er en av de positive sidene ved outsourcing. Én informant [D] beskriver det som «*vi er jo litt generalister. Vi skal kunne alt om alt, og i praksis blir det ingenting om alt*». Samtidig er det flere som trekker frem innleie av spesialister dersom det skulle være behov.

Ved å outsource IKT-tjenester til andre aktører fordrer det at virksomheter også har kompetanse til å følge opp tjenesteleverandøren (Justis- og beredskapsdepartementet, 2016a; NOU 2015:13). Bestillerkompetanse og oppfølgingsansvar er fraværende hos informantene, som kan tyde på at de ikke anser det som en risiko eller som nødvendig. Det er tidligere påpekt at operatører har et selvstendig ansvar og må forsterke oppfølgingen av leverandører, for å styrke sikkerheten (Arbeids- og sosialdepartementet, 2018). Tilgang til ekspertise virker å være av betydning for fire av informantene, der outsourcing samtidig bidrar til et redusert behov for å bygge opp kompetanse innad i eget selskap. Flere begrunner dette med at IT ikke er kjerneaktiviteten deres. Å miste kompetanse virker ikke å være av stor bekymring hos informantene. Dette kan ofte være et bevisst valg fra virksomheters side (NOU 2015:13). Tilgang til dybdekompetanse på ulike områder fremheves som en medvirkende faktor for å velge outsourcing. Imidlertid påpekes det av enkelte informanter at kompetansen bør innebære kunnskap og forståelse om bransjen, og som er en faktor som påvirker valg av lokal tjenesteleverandør.

Risikovurdering

Risikovurderinger skal være en integrert del av helhetsvurderinger (NSM, 2017a), og en integrert del i risikostyringsprosesser. Virksomheter har et selvstendig ansvar for å identifisere egne verdier og sårbarheter (Justis- og beredskapsdepartementet, 2016b). Dette er nødvendig for å kartlegge hvilket sikkerhetsnivå som er tilstrekkelig for IKT-tjenestene, noe som avgjøres etter gjennomført risikovurdering. For å ha nødvendig sikkerhetsnivå må virksomheter se på helheten, som innebærer både tekniske, organisatoriske og administrative tiltak så vel som de trusler man ønsker

beskytte seg mot (NOU 2015:13). Når det gjelder risikovurderinger i forbindelse med outsourcing er det varierende gjennomførelse av dette hos operatørselskapene. Av de syv operatørene som har outsourcet, er det fire som ikke har risikovurdert dette, enten ikke i det hele tatt eller ved nye anbudsrunder. De to som ikke outsourcer har foretatt enkle vurderinger og har betraktet den totale risikoen som for høy. At så få gjennomfører risikovurderinger er oppsiktsvekkende, da risikobildet i økende grad forverres (NSM, 2017a). IKT-sikkerhet handler om å være bevisst på hva og hvem man ønsker å beskytte seg mot, der risikovurderinger og andre analyser kan gi oversikt over sårbarheter og egen sikkerhetstilstand (NOU 2015:13; NSM, 2017a).

Risikovurderinger må gjennomføres ved bruk av underleverandører, og bør inkludere behandling, skjerming og lagring av informasjon samt tjenesteleverandør. Ved bruk av nye tjenesteleverandører er det spesielt viktig å risikovurdere terminering av kontrakter, tilbakeføring eller flytting av informasjon, og destruksjoner av lagringsmedium (NSM, 2017a). At fullverdige vurderinger ikke er gjennomført er interessant, spesielt sett mot den risikoen outsourcing medfører. Det viser seg ofte at risikovurderinger ved tjenesteutsetting ofte er mangelfulle eller fraværende, der IKT-tjenester outsources uten sikkerhetsfaglige vurderinger i forkant (NOU 2015:13; NSM, 2017b; NSM, 2018). Dette er en problemstilling som ses i flere sektorer. Således kan det reflekteres over hvorfor dette er en gjennomgående utfordring. At få av informantene har gjennomført fullverdige risikovurderinger, med tilhørende risiko- og sårbarhetsanalyser, er bemerkelsesverdig. Spesielt siden det er syv som har valgt outsourcing i ulik skala. Det faktum at flertallet ikke har gjennomført risikovurderinger gir indikasjoner på at dette ikke er signifikant i deres vurderinger.

Black swans

Tjenesteutsetting øker sårbarhetsflaten og risikoen til virksomheter, ved at det blir et større antall underleverandører. Manglende kontroll over risiko i informasjonssystemene som følge av utilstrekkelig risikostyring er en alvorlig sårbarhet, der petroleumssektoren er spesielt utsatt grunnet økende risiko for industrispionasje og produksjonsstans (NSM, 2018; NUPI, 2018). På bakgrunn av dette er det nødvendig at risikovurderinger inkluderer ukjente, men alvorlige trusler. Eksplosjonen i oljerørledningen i Erzincan eksemplifiserer dette, der årsaken var hackerangrep. Blant informantene er det bred enighet om at slike risikoer ikke kan forhindres, der én informant forteller at *«IT-sikkerhet er ikke å hindre at noen kommer inn, det klarer du aldri. Det er bare å forsinke, og ha mekanismer som gjør at det blir oppdaget på vei inn»* [Informant H]. Derimot er

det en stor variasjon i hvordan informanter håndterer ukjente risikoer, forholdsvis ut fra en barrieretilnærming. Likevel er det ingen som betrakter ukjente risikoer som en faktor ved outsourcing.

Tilgang til eksterne tjenester

Ved å benytte én leverandør kan man minimere risikoen og begrense skadeomfanget ved hendelser (NOU 2015:13). Fåtallet av informantene presiserer at de ønsker én stor tjenesteleverandør, heller enn flere, da de ønsker å få dekket mest mulig av IKT-porteføljen sin. I tillegg er det flere som mener det kan gi bedre sikkerhet gjennom tilgang til dybdekompetanse og overvåkingstjenester. Sistnevnte virker å være av relevans, da fire informanter forteller at de av overvåkning på nettverket deres. Tre av disse outsourcer IKT-tjenester, og får dette levert av tjenesteleverandør. I den sammenheng er det enkelte som har vektlagt leverandør ut fra krav om dette. Gjenværende informant forteller å overvåke nettverket selv. Det kan trekkes frem at NSM også tilbyr overvåkningstjenester, men kun dersom virksomhetene selv inngår en avtale for å få tilgang til tjenesten (NUPI, 2018).

Oppsummering av interne faktorer

Faktorer kategorisert som interne er gjennomgått, med det formål å se om de har hatt betydning for vurderingene rundt outsourcing. Det viser seg at fordeler som kan knyttes til tilgang på kompetanse og fokus på kjernevirksomhet er av betydning i ekspertenes vurderinger, der risiko ved de samme fordelene ikke vektlegges i like stor grad. Spesielt henvises det til egen bestiller- og oppfølgingskompetanse. Samtidig argumenteres det for at man får bedre sikkerhet ved å knytte seg til fagmiljøer som har spisskompetanse på IKT, særlig om de har bransjeforståelse. Ved å tilegne seg kompetanse på IKT, i tillegg til overvåkingstjenester, betraktes dette å redusere risikoen for hendelser.

Generelt kan det trekkes konklusjoner til at interne faktorer som gir fordeler knyttet til økonomi og drift veier tyngre i eksperters vurdering av outsourcing. Det er lav gjennomføring av fullverdige risikovurderinger knyttet til å tjenesteutsette IKT-tjenester, noe som kan føre til mangelfullt risikobilde for operatørene. Dette er en utfordring som er sektoruavhengig, og således en kjent problematikk. Man kan derfor stille spørsmål ved hvorfor det ikke gjennomføres. På bakgrunn av

dette kan det være vanskelig for ekspertene å argumentere mot outsourcing, sett fra et større perspektiv der eksterne faktorer også trekkes inn i vurderingene.

5.2.2 Eksterne faktorer

Internasjonale virksomheter

Petroleumsbransjen er i stor grad internasjonal, der operatører er både norske og utenlandske. Flere er del av større globale konsern som legger føringer for drift (NOU 2015:13). Syv av operatørene er del av internasjonale selskap, som varierer i størrelse og geografisk beliggenhet. Av disse er det fem som nevner at det har vært press mot å outsource fra det globale miljø, av ulike årsaker som forventning og standardisering av prosesser. For én av informantene var årsaken til outsourcing et ønske om samme sikkerhetsnivå på de ulike lokasjonene. Flere understreker at outsourcing ikke var et valg, men et krav satt av det globale selskapet. Enkelte har ikke hatt mulighet til å velge outsourcingsmodell og tjenesteleverandør selv. Andre har opplevd press mot outsourcing til lavkostnadsland, dog har etter egne vurderinger fått velge leverandør selv. Dette er blant store internasjonale selskaper, der avtalen med tjenesteleverandør også er av internasjonal karakter. På en annen side er det to informanter som forteller at outsourcing aldri har vært et valg, men en selvfølge. Dette fremstilles som en forventning fra de globale selskapene de er en del av, men har i større grad hatt påvirkning på valg av tjenesteleverandør og outsourcingsmodell.

Det er enkelte virksomheter som ofte har et sikkerhetssamarbeid med det globale selskapet (NOU 2015:13), der to informanter forteller at det internasjonale selskapet har gjennomført vurderingene når det gjelder outsourcing. Flere informanter nevner at de har standardiserte risikostyringsprosesser globalt, der det understrekes å være stort fokus på IKT-sikkerhet. Dog er det da interessant at de fem informantene som ikke har gjennomført analyser lokalt, er de samme som har opplevd press fra det globale konsern. Dette viser seg å ha påvirkning når det gjelder valg av outsourcing, der mangel på lokale analyser har hatt redusert mulighet til å påvirke valg av outsourcingsmodell og tjenesteleverandør. Operatørene som er en del av internasjonale selskaper har i liten grad påvirkning på hvorvidt de outsourcer, der de globale vurderingene derimot kan være av betydning for outsourcingsmodell.

Læring av hendelser

Tidligere uønskede hendelser utgjør et viktig læringsgrunnlag, både de som inntreffer i egen virksomhet eller andre (NSM, 2017a). Samtidig er det et viktig moment når det kommer til vurderinger vedrørende outsourcing, og eventuelt valg av modell og tjenesteleverandør. Dette er fordi det kan gjøre operatører mer robuste i møte med samtidens utfordringer og trusler. Imidlertid ser man at konsekvenser som følger av uønskede hendelser fører til at virksomheter er restriktive med å være åpne om hendelser, i den forstand at de ikke ville gått ut med det (NSM, 2017a). Tre informanter understreker at de aldri hadde gått offentlig ut med IKT-relaterte hendelser i sin virksomhet, hvor det bemerkes at det er de samme tre som har vektlagt omdømme i sin vurdering når det gjelder outsourcing. Hemmelighold rundt hendelser fratar operatører muligheten for læring, samt at den preventive effekten når det kommer til IKT-sikkerhet begrenses. På bakgrunn av dette oppfordres virksomheter til å dele informasjon om hendelser med hverandre, nettopp for å legge til rette for læring i egen virksomhet og hos andre (NSM, 2017a).

En av de informantene som ikke ville offentliggjort egne hendelser forteller at det er bra at andre operatører er åpne om hendelser, og henviser til angrepet hos Maersk i fjor sommer. Informanten påpeker at dette er viktig for deres læring og oppmerksomhet rundt risiko. Her bemerkes det at dersom hendelser ikke skjer, vil det være vanskelig å få tilstrekkelig oppmerksomhet hos ledelse. Tilsvarende belyses også i NUPI (2018), som viser at manglende hendelser legger føringer for økonomisk støtte til IKT. Åpenhet om hendelser vil føre til aksept og forståelse av behovet for god informasjonssikkerhet, og samtidig legge til rette for en god åpenhetskultur (NSM, 2017a). Derimot setter flere operatører omdømme fremfor åpenhet. Tidligere hendelser virker å bli benyttet til å få mer ressurser, men har imidlertid ikke effekt på valg av outsourcing.

Lovverk og standard

Det virker som få informanter vektlegger retningslinjer eller standarder som føring for deres valg når det kommer til outsourcing. Imidlertid nevner noen få informanter ISO-standarder som et krav hos tjenesteleverandør. Hvilke lover og regler som gjelder for sektoren nasjonalt og internasjonalt er noe som bør fremkomme i vurderingene ved tjenesteutsetting (NSM, 2017a). To av informantene fremhever at General Data Protection Regulation (GDPR), som er den nye personvernforordningen som har forventet ikrafttredelse juli 2018, har stort fokus innad i operatørselskapene. Begge begrunner dette som en mulighet til å få orden i systemene. Én av

informantene sier at dette har en direkte betydning for valg av tjenesteleverandør, spesielt når det kommer til lokasjon. Operatøren benytter nå en tjenesteleverandør utenfor landets grenser, der den nye personvernloven kan være et insentiv for å presse frem en lokal tjenesteleverandør. Informanten [G] forteller at «*[...] det har det også vært vurdert andre land utenfor EU. Nå i senere tid så er det stort sett GDPR som vi bruker, og sier bare legger det død da*».

Risikoforståelse

Sikkerhetstilstanden til en virksomhet påvirkes av kunnskap om egne verdier, samt forståelse for at verdiene er attraktive for ulike trusselaktører. Hvordan man forholder seg til dette er avgjørende for egen risikoerkjennelse, i tillegg til at det er viktig for å ta gode beslutninger (NSM, 2017b). Som tidligere nevnt er informantene generelt lite bevisst på operatørselskapenes verdier, der én informant belyser en gjennomgående utfordring:

> «*Det som er vesentlig er på en måte at de som eier data forstår det ansvaret. Og det er også et tiltak vi har innenfor datasikkerhet, nemlig at dataeier, og da tenker jeg på en direktør på rett nivå forstår hva det er han eier, og at den personen er med og lytter til den beslutningen de anbefaler, for da vet de hva som skjer med dataene sine*» [Informant F].

Informanten mener det må bli en større bevissthet på hvilket ansvar man har, og hvilken kompetanse som er nødvendig for å ivareta informasjonssikkerhet. Imidlertid ses et manglende fokus på verdier og risiko ved outsourcing. Selv ved manglende risiko- og sårbarhetsvurderinger *«[...] mener de fleste av virksomhetene at egen sikkerhetstilstand er «god». Grunnlaget for å fremsette den påstanden er ikke alltid like solid»* (NSM, 2017b:24).

Tross at informantene fremstår å være fornøyd med eget arbeid i forbindelse med informasjonssikkerhet, oppgir flertallet som outsourcer at de selv ville valgt en annen type outsourcingsmodell og/eller tjenesteleverandør. En informant peker eksplisitt på at det optimale var dersom de selv hadde styring internt i selskapet, heller enn å bli styrt av det internasjonale konsernet. Tjenesteutsetting krever riktig beslutning på riktig nivå, der risikoforståelse kan være grunnleggende for valg av beslutning (NSM, 2017b; NSM, 2018).

Oppsummering av eksterne faktorer

Eksterne faktorer er inkludert for å undersøke hvorvidt de er av betydning for risikovurderingene og beslutninger når det kommer til outsourcing. Enkelte av de overnevnte faktorene utgjør rammebetingelser og krav for operatørene, og påvirker de valg som tas. Spesielt vesentlig er press fra internasjonale selskap, som legger føringer for operatørenes autonomi når det gjelder outsourcing. Når det kommer til GDPR velger enkelte operatørselskaper et strategisk valg der de bruker loven til å få gjennomslag for lokal tjenesteleverandør. Slik sett bruker de rammebetingelser for å oppnå fordeler, noe som kan bidra til mer kontroll der man reduserer utfordringer som følge av kulturelle forhold.

En faktor som fremkommer spesielt interessant er læring. Dette er på grunn av faktorene som i stor grad kan benyttes til å redusere risikoer, da det bidrar til økt kunnskap og kompetanse. Et paradoks er at det uttrykkes ønske om å dele erfaringer for å sikre kunnskapsoverføring, samtidig som flere av operatørene ikke ville gått ut med egne hendelser. Begrunnelsen her er omdømme, noe som står sterkt i vurderingene. Mange av valgene som gjøres i relasjon til outsourcing, tilsier at det er en manglende risikoforståelse. Dette kan være fordi det er flere faktorer som de selv ikke har kontroll over, og som legger føringer for beslutninger. Flere av informantene fremhever dette, der de uttrykker et ønske om en annen outsourcingsmodell og/eller tjenesteleverandør.

5.3 Hvordan påvirker læring og styring i sektoren operatørers vurderinger når det gjelder informasjonssikkerhet?

Forskningsspørsmålet har som formål å undersøke hvordan læring og styring i sektoren påvirker operatørenes vurdering vedrørende outsourcing. Dette inkluderer både mellom virksomheter, samt mellom eksterne aktører og virksomheter. I den forbindelse vil eksterne aktører innebære fagdokumenter fra blant annet NSM og NUPI. Når det gjelder styring har det vært fokus på Ptil som tilsynsmyndighet, og deres rolle i forbindelse med informasjonssikkerhet.

5.3.1 Læring

Operatører i petroleumssektoren er stadig mer sårbar og utsatt for nye risikoer, som forsterkes ved outsourcing av IKT-tjenester. Det har tidligere blitt gjennomgått hvordan eksperter vurderer denne risikoen og hvilke kriterier som vektlegges i deres vurderinger. Et element som kan påvirke

risikoforståelse og beslutninger er hvordan operatører lærer etter digitale hendelser, spesielt som følge av outsourcing. Kapittelet legger vekt på læring og styring mellom virksomheter og fra eksterne aktører. I denne sammenheng er eksterne aktører eksempelvis NSM, NorCERT og PST.

Læring i egen virksomhet

Det er viktig at virksomheter identifiserer og lærer av egne handlinger, slik at kunnskapen og erfaringen ikke forsvinner. For å opprettholde god sikkerhet er det viktig å oppdage forbedringspunkter, eksempelvis når det gjelder sikringstiltak og/eller planverk (NSM, 2017b). Petroleumssektoren er stadig mer utsatt for digitale sårbarheter (NOU 2015:13), og samtlige av informantene forteller om digitale uønskede hendelser, men i varierende grad. De fleste hendelser er av mindre alvorlig karakter, og har ikke hatt større negative konsekvenser for operatørene. Likevel har enkelte operatører iverksatt ulike læringstiltak innen informasjonssikkerhet, med fokus på bevisstgjøring av brukerne. Dette begrunnes med at mennesker ofte er det svakeste punkt, i tillegg til at det fortelles om en økende trend innenfor ulike svindelforsøk og phishing.

Enkelte virksomheter har tilrettelagt for å registrere sikkerhetstruende hendelser, men det viser seg at hendelser ofte ikke blir rapportert. Dette gjør det vanskelig å lære av tidligere hendelser, og kan tyde på lav bevissthet rundt sikkerhet (NSM, 2017b). Antakeligvis er det store mørketall når det gjelder rapportering i virksomheter (NSM, 2017b). Årsaker til manglende rapportering av hendelser kan skyldes at det er store gråsoner, eksempelvis at det ikke er tydelig definert i lov eller at operatørene ikke anser trusler og/eller angrep som alvorlig. Det kan også handle om frykt for omdømme, tilsyn eller at det fører til nye sikkerhetstiltak og forstyrrelser av daglig drift (NOU 2015:13; NUPI, 2018). Underrapportering kan føre til manglende åpenhet og erfaringsutveksling vedrørende digitale trusler og hendelser, som forårsaker at samarbeidet i sektoren ikke er optimalt (NOU 2015:13).

Læring mellom virksomheter

Virksomheter har ansvar for hvordan egne handlinger kan påvirke andres sikkerhet (Justis- og beredskapsdepartementet, 2016b). Åpenhet omkring hendelser kan bidra til læring hos seg selv og andre, og erfaringer bør deles og kommuniseres til relevante interessenter (Justis- og beredskapsdepartementet, 2016a; NSM 2017c). Det er tidligere påpekt god kunnskaps- og erfaringsutveksling mellom virksomheter, spesielt rundt HMS, som legger til rette for god læring

(Arbeids- og sosialdepartementet, 2018). Det fremkommer imidlertid at ekspertene ikke er interessert i informasjonsdeling mellom operatører når det kommer til sikkerhetsrelatert informasjon, uavhengig av kritikalitet. Et interessant element er at kunnskapsdelingen indikeres å være ulik mellom HMS og IKT-sikkerhet. For å kunne forebygge uønskede hendelser må læring være en integrert del av virksomhetens arbeid, og ikke et konkurrerende hensyn (Justis- og beredskapsdepartementet, 2016b). Virksomheter er avhengig av sitt internasjonale nettverk og selskap når det gjelder å få tak i informasjon som er nødvendig for trusselbildet. Mangelfull læring mellom virksomheter kan påvirke hvordan man forstår risikoene, og dermed forholder seg til risikobildet. Følgelig kan det ha innvirkning på gjennomføringen og utviklingen av risikovurderingene. Informasjonen som kommer fra andre virksomheter, gjerne internasjonale, vektlegges gjerne mer enn informasjonen som kommer fra myndigheter (NUPI, 2018). Dette kan være forårsaket av manglende IKT-kompetanse hos myndigheter, der det heller ikke gjennomføres tekniske tilsyn sett mot IKT i bransjen (Justis- og beredskapsdepartementet, 2016b).

Gjensidig avhengighet

Petroleumssektoren har komplekse infrastrukturen, der det er en stor integrasjon med flere partnere, har ført til en kompleks og gjensidig avhengighet mellom virksomheter, leverandører og underleverandører. Kompleksiteten medfører at digitale systemer må være pålitelig og sikre, samt ivareta informasjonssikkerheten (IRIS, 2018; NOU 2015:13). Et komplekst aktørbilde forsterker sårbarheten i verdikjeden, der det blir stadig vanskeligere å beskytte systemer (IRIS, 2018; NSM, 2017a). Flere av informantene forteller at de ble direkte påvirket av hendelsen til Maersk, både i forbindelse med tilgang til data og risikoreduserende tiltak. Således illustrere dette avhengigheten mellom virksomheter i sektoren. Denne forsterkes ved outsourcing, da virksomhetene stadig blir mer avhengig av underleverandører for å oppdage, redusere og håndtere hendelser (IRIS, 2018).

Samhandling

Informasjon i forbindelse med hendelser i sektoren er viktig for å kunne forhindre at liknende hendelser skjer igjen (NUPI, 2018). Informantene forteller om lite samarbeid mellom virksomhetene, og det er heller ikke opprettet et felles responsmiljø. Lite samarbeid utfordrer kommunikasjon og informasjonsflyt i sektoren, og det bør etableres et initiativ for digitalisert samhandling i sektoren. Dette åpner for muligheter for datadeling og tilgang mellom aktører i næringen, noe som kan innebære forbedring og effektivisering av Ptils virksomhet (KonKraft,

2018). Informantene er delt hvorvidt det er behov for et fagmiljø for informasjonssikkerhet. Dog uttrykkes det et behov blant flere informanter om at Ptils rolle bør styrkes, der det reflekteres over om Ptil er inne i en læringsfase når det kommer til IKT-sikkerhet og om de per i dag er kompetent nok. For at et funksjonelt regelverk skal fungere, understrekes det behov for god samhandling, dialog og tillit mellom virksomheter og myndigheter (Arbeids- og sosialdepartementet, 2018).

Læring mellom virksomhet og eksterne aktører

Petroleumssektoren er påpekt å ha god erfaring med læring, blant annet gjennom etablerte fora på myndighetsnivå og trepartssamarbeidet (Arbeids - og sosialdepartementet, 2018). Dette er imidlertid tvetydig, da det av andre påpekes å være en utfordring med informasjonsdeling mellom virksomheter og eksterne aktører (NUPI, 2018). Ved uønskede hendelser er det nødvendig å handle på nasjonalt og internasjonalt nivå når det kommer til å styrke IKT-sikkerheten (NSM, 2017a; Justis- og beredskapsdepartementet, 2016b). Når det gjelder sikkerhetsarbeidet i sektoren er det bekymringer knyttet til både variasjon i arbeidet og hvorvidt små selskaper er godt nok rustet for et godt IKT-sikkerhetsarbeid (NUPI, 2018). Det viser seg å være et tvetydig behov når det kommer til mer retningslinjer i forbindelse med digital sikkerhet. Enkelte informanter uttrykker behov for tydeliggjøring vedrørende hva de har å forholde seg til, mens andre mener det foreligger mer enn nok. Det ses at de som oppgir å ha et behov er fra mindre operatørselskap. For å kunne håndtere hendelser effektivt er det nødvendig med god informasjonsdeling mellom virksomheter og myndigheter, der de er gjensidig avhengig av hverandre (NUPI, 2018).

Petroleumstilsynet reflekterer rundt hvorvidt de skal etablere en felles arena på vegne av sektoren, der det legges til rette for læring vedrørende digitale sårbarheter og trusler. Det trekkes frem at internasjonale selskap har et godt apparat i ryggen, og sektoren har et flertall av disse som operatører. Dermed er det de mindre virksomhetene som har størst nytteverdi av dette. Samtidig påpeker Ptil at det er en manglende entusiasme når det kommer til deltakelse på seminar som omhandler tematikken, der eksempelvis NSM og NorCERT holder foredrag. Det påpekes også at alvorlighetsgraden ved hendelser varierer, der store selskap gjerne påfører større konsekvenser, som også kan gå ut over samfunnet generelt sett. Det er likevel tidligere påpekt at det er behov for bedre systematisering av kunnskap for å lære, både av uønskede hendelser og det som er bra, for å forebygge at hendelser inntreffer (Arbeids- og sosialdepartementet, 2018).

Oppsummering av læring

Læring og kunnskapsdeling kan ha stor påvirkning på hvordan operatørene vurderer risiko, fordi kunnskap om digitale sårbarheter og risikoer legger grunnlaget for å ta velinformerte beslutninger. Det viser seg at mindre operatører har et større behov for informasjon og retningslinjer enn de store internasjonale selskapene. Dette ser man også ved håndtering av hendelser, der store operatører ofte har egne responsmiljø. Det er få som ønsker å dele informasjon med hverandre, og således dannes det ikke et godt grunnlag for læring av hverandre. Videre fremkommer det et lavt engasjement når det gjelder å delta på seminar som omhandler informasjonssikkerhet.

På grunn av sterk gjensidighet mellom oljevirksomheter og underleverandører påvirkes operatører lettere av hendelser som skjer hos andre. Dette har man sett eksempler på tidligere, og bør være en motivator for å styrke samhandlingen innad i sektoren. Petroleumstilsynet reflekterer over hvorvidt det skal være deres ansvar, og om det er sektoren i sin helhet som har behov for dette. Det påpekes at en felles arena også vil bidra til effektiv hendelseshåndtering, spesielt fordi alvorlige hendelser gjerne krever bistand fra eksterne, blant annet NSM og NorCERT. Således kan det argumenteres for at det vil være fordelaktig å benytte seg av felles kompetanse til å forebygge, heller enn å håndtere.

5.3.2 Styring

Ved outsourcing av IKT-tjenester bør risikostyring være en integrert del av virksomheters kjerneprosess (NSM, 2017b). Digitalisering skaper utviklingsmuligheter, så vel som utfordringer som er grenseoverskridende. Disse går på tvers av sektorer og virksomheter, dels utenfor myndigheters kontroll. For å kunne styre utviklingen og redusere risiko vil tiltak og strategiske valg fra myndighetenes side være avgjørende (IRIS, 2018; NSM, 2018). Styring i sektoren kan påvirke hvilke handlingsrom og muligheter operatørene har, og utgjør således en viktig faktor som må tas i betraktning for å forstå eksperters vurderinger ved outsourcing.

Risikostyring

NSM, Politiets sikkerhetstjeneste (PST), Etterretningstjenesten (E-tjenesten) og DSB lager årlige vurderinger av forhold som kan true norske verdier eller interesser som man ønsker å beskytte. Disse kan være et viktig bidrag til risikostyringen i sektoren og hos virksomheter, med det formål at risikoforståelsen bedres (Justis- og beredskapsdepartementet, 2016b). Manglende forståelse kan

påvirke risikopersepsjonen, som videre kan føre til feil oppfattelse av risiko (IRIS, 2018). Imidlertid ser man at effektiv hendelseshåndtering og risikostyring er mangelvare. Dette fører til manglende kontroll over risiko og utgjør en sårbarhet, som forsterker behovet for grundige risikovurderinger slik at gode tiltak iverksettes (NSM, 2018). Selv om sektoren har større integrasjon av digital teknologi har det imidlertid ikke vært endringer i metodikk når det gjelder håndtering av risiko. Risikostyring er nødvendig både i virksomhetsstyringen (NSM, 2017b), i tillegg til at integrerte operasjoner krever indirekte styring av risiko ved ulike prosessfaser (IRIS, 2018). Det er påpekt at risikostyring på myndighetsnivå bør forbedres. Dette gjelder blant annet gjennom revisjoner av verdikjedene og vurderinger når det gjelder risikoreduserende strategier. Videre fremheves et behov for bedre samarbeid og kunnskapsdeling mellom eksperter innen HMS og IKT (IRIS, 2018).

Tilsyn

Mer teknisk kompleksitet når det kommer til IKT øker utfordringene på tilsyn (NOU 2015:13), der det er påvist at flere tilsynsmyndigheter har behov for å bygge opp kompetanse innen IKT (DNV GL, 2018; Justis- og beredskapsdepartementet, 2016b). Det er påpekt at Ptil har behov for mer teknisk kompetanse innen IKT og digitale systemer for å kunne gjennomføre fullverdige tilsyn. Samtidig er det pekt på at det bør etableres felles retningslinjer og standarder for å ha klare rammer å jobbe ut fra (IRIS, 2018). Samtidig ser man at det er uklarheter om det er mulig å bygge opp tilstrekkelig kompetanse (Justis- og beredskapsdepartementet, 2016b). Samtlige informanter forteller at de har hatt tilsyn fra Ptil de siste årene når det gjelder IKT, som alle har en entydig forståelse om at det ikke er direkte tilsyn. Informantene har karakterisert det som «en samtale», «en presentasjon» eller «tilsyn light», der flere reflekterer over om dette var for Ptils egen læring og hvor ingen har fått oppfølging i etterkant. En informant forteller i den forbindelse at de har for få retningslinjer å gå etter ved tilsyn, og at «*de har ikke noe lovverk å slå i bordet med*» [Informant B]. Dette bekreftes av Ptil, og begrunnes med at tekniske krav i innretningsforskriften ikke har tilbakevirkende kraft. Derfor kan det bare gjøres tilsyn på generell basis.

Imidlertid er det gjort tilsyn basert på NOG 104, tross manglende lovhjemmel for dette, uten at dette førte til negative reaksjoner fra operatørene. Dette indikerer at operatørene setter pris på medvirkning fra Ptil på området. Det fremkommer også at tilsyn spisser fokuset på de områdene

som Ptil vektlegger, der: «*vi ser er at når vi har fokus på et område, så reagerer næringen*» [Informant J]. En generell utfordring er at dersom regelverk ikke henger med i den tekniske utviklingen vil det være lite å utøve tilsyn etter (NOU 2015:13). Da tilsyn er sektorspesifikk og kontrollerer at virksomheter har et styringssystem eller internkontrollsystem på plass når det gjelder informasjonssikkerhet er det nødvendig med kunnskap for effektive og målrettede tilsyn (Justis- og beredskapsdepartementet, 2016b). Det som differensierer petroleumssektoren fra andre sektorer er at ansvaret for IKT-sikkerhet ligger hos operatørene. Petroleumstilsynet presiserer at «*det er operatøren som er den ansvarlige, og som skal finne de løsningene som er tilfredsstillende og ha evne til å håndtere situasjonen*». Ptil sin rolle er å følge opp at operatørene selv tar ansvar.

Helhetlig tilnærming

Når det gjelder informasjonssikkerhet er det flere regelverk som pålegger virksomheter å ha et styringssystem (Justis- og beredskapsdepartementet, 2016a). Det belyses ofte viktigheten med å ha styringssystem for informasjonssikkerhet for å kunne redusere digital sårbarhet. Krav, føringer og måloppnåelse i relasjon til informasjonssikkerhet bør også inngå i den generelle etatsstyringen (NOU 2015:13). NSM anbefaler å basere sikkerhetsarbeidet på anerkjente standarder, eksempelvis ISO27000-serien. Ved å legge til grunn ISO-serien knyttes sikringstiltak opp mot virksomhetens risikostyring, noe som gir en helhetlig tilnærming til beskyttelse av risikoutsatte verdier (NSM, 2017b). Samtlige informanter, bortsett fra én, forteller at ISO-standarder er integrert i deres standard og/eller styringssystem. Som tidligere nevnt er etterlevelse av ISO også vektlagt av enkelte hos tjenesteleverandør. Selv om det ikke eksisterer en overordnet lov for IKT-sikkerhet, så utvikles det stadig flere standarder når det kommer det informasjonssikkerhet. Dette er hensiktsmessig fordi det øker kvaliteten på informasjonssikkerhetsarbeidet (NOU 2015:13). For petroleumssektoren kan dette være svært nyttig, da det stilles spørsmål ved om det eksisterende rammeverket i petroleumssektoren, med tilhørende metoder og prinsipper for risikostyring, er gode nok (IRIS, 2018).

Den digitale trusselen mot petroleumsbransjen har eksistert over tid, der økende systemintegrasjon forsterker denne trusselen. Spesielt viser det seg at sektoren er stadig mer utsatt for hackerangrep, eksempelvis ble sektoren utsatt for et alvorlig spionasjeangrep i 2014 (Forsvarets forskningsinstitutt, 2016; NOU 2015:13). For å redusere digitale sårbarheter er det nødvendig med god IKT-sikkerhet, inkludert lovverk som bidrar til dette arbeidet. Det er foreslått at det stilles krav

til at virksomheter beskytter sine verdier (NOU 2016:19). Videre anbefales det at departementene tydeliggjør krav og føringer i virksomhetsstyring, der tilsynsmyndigheter må følge opp dette (NOU 2015:13). Det er et fåtall av informantene som mener det ikke er behov for mer lovverk rundt IKT-sikkerhet, der én oppgir å være *«usikker på om det er lovverk og reguleringer som er veien å gå når det gjelder å sikre sine verdier»* [Informant G].

Imidlertid reflekterer flere av informantene over hvorvidt dagens regelverk er godt nok, der enkelte mener det er for svakt når det kommer til IKT-sikkerhet. Et interessant utsagn som kommer fra en informant, sier at «*det holder det som er bransjestandard og best practice fra de forskjellige leverandørene*» [Informant E]. Paradokset her er at man da er prisgitt outsourcing, noe ikke alle i bransjen gjør. Det er også belyst at IKT-sikkerhet er en av hovedutfordringene knyttet til risiko i bransjen (IRIS, 2018). Det er påpekt at man bør vurdere om dagens regelverk rundt IKT-sikkerhet er hensiktsmessig og tydelig nok for å kunne ivareta de nye digitale samfunnsutfordringene (Justis- og beredskapsdepartementet, 2016a). Behovet for oppdatering av regelverk og standarder blir stadig mer fremtredende. Spesielt trekkes dette frem ved implementering av ny teknologi og digitalisering, som også vil påvirke hvordan sektoren følges opp i fremtiden (Arbeids- og sosialdepartementet, 2018; KonKraft, 2018).

Operatørene har flere regelverk å forholde seg til, der noen er sektorspesifikke og andre sektorovergripende (Justis- og beredskapsdepartementet, 2016a). Det er tvetydighet knyttet til regelverk og tilsyn blant informantene, som tolkes dit hen at det er lite føringer og beslutningsstøtte når det gjelder IKT og outsourcing. Styring og tilsyn fra Ptil indikeres å ha en liten innvirkning på beslutning når det gjelder outsourcing, i tillegg til at operatørene står relativt fritt til å handle ut fra egeninteresser. Regulering gjennom lov og forskrift er blant myndighetenes sterkeste virkemidler, og må brukes bevisst. Spesielt fordi dagens risikobilde viser at utfordringene er tverrsektorielle, som krever en helhetlig tilnærming (Justis- og beredskapsdepartementet, 2016a).

Oppsummering av styring

Styring er viktig når det kommer til IKT-sikkerhet fordi det legger føringer for hva som aksepteres av risiko knyttet til informasjonssikkerhet. Det bidrar til å danne rammene for operatørene, og legger grunnlag for handlingsvalg. Således vil dette påvirke hvordan operatører forholder seg til risiko knyttet til outsourcing av IKT-tjenester. Med fordel kan risikostyringen både i sektoren, og

innad i virksomhetene, bedres. Dette begrunnes med at risikostyring i relasjon til IKT i sektoren påvirker muligheter og valg hos operatørselskapene.

Det viser seg at Ptil har stor innvirkning på de områdene som operatørene får varslet tilsyn på, der næringen reagerer ved å sette fokus på de områdene. Dette viser at tilsyn har en direkte påvirkning på hvordan operatører jobber med informasjonssikkerhet. Følgelig kan bedre styring gi bedre beslutningsgrunnlag for operatører når det kommer til informasjonssikkerhet og outsourcing. Petroleumssektoren skiller seg fra andre sektoren ved at det er mer ansvar hos operatørene, noe som kan kreve mer styring gjennom tilsyn og regulering.

6. Diskusjon

I dette kapittelet vil studiens empiriske funn ses i lys av studiens teoretiske perspektiver. Kapittelet er strukturert etter forskningsspørsmålene, og utgjør dermed 3 delkapitler. Analysen trekker frem hovedelementene av studiens funn, der disse utgjør underoverskrifter, før det avslutningsvis under hvert delkapittel vil være en oppsummering av de mest fremtredende funnene.

6.1 Hvordan forstår eksperter risiko og sårbarhet knyttet til outsourcing, og hvordan vektlegges dette i risikovurderinger?

Ved outsourcing av IKT-tjenester er det kritisk med robust risikostyringsprosess, der virksomheter må identifisere og anerkjenne risiko (Aris et al., 2008; Prado, 2011; Samantra et al., 2013). Dette er fordi man skal kunne balansere konflikterende hensyn, der risiko og sikkerhet må vurderes opp mot fordeler, som eksempelvis økonomi og konkurransedyktighet (Aven, 2010; Aven, 2015a). I studien er det identifisert flere risikofaktorer som eksperter vurderer i forbindelse med outsourcing, men som vektlegges forskjellig. Imidlertid bemerkes det at risikoen i mindre grad anerkjennes, og at mer fordelaktige hensyn tas.

Tidligere forskning viser at kostnadseffektivitet er en hovedårsak til at virksomheter velger outsourcing av IKT (Fell, 2013; Oshri, 2011). Det blir ofte sett på som nødvendig, spesielt i miljøer som er preget av globalisering og konkurranse (Fan et al., 2012). Derimot anser flere eksperter kostnad som en risiko, på grunn av skjulte kostnader gjennom stor turnover og lav kvalitet på tjenestene. Dette gjelder outsourcing til lavkostnadsland. I tillegg utsettes underleverandører for stadig flere angrep (NSM, 2017b), der sikkerhetsbrudd vil føre til økte kostnader (Cezar et al., 2014). Det er likevel få som vektlegger dette i vurderingene sine. Det er interessant at ekspertenes forståelse av kostnad motstrider tidligere forskning og fagdokumenter. Dette kan forekomme av at ulike interessenter har forskjellig oppfattelse av risikoer (Qi et al., 2012).

Verdier og omdømme

Når virksomheter vurderer å outsource anbefales det å vurdere hvilke verdier de har, slik at de kan beskytte og ha kontroll over dem (NSM, 2017a; NSM, 2017b; NSM, 2018). Dette er fordi outsourcing forhøyer risikoen for at informasjon kommer på avveie eller blir eksponert. Det er indikasjoner på at ekspertene ikke ser på dette som bekymringsverdig, selv om det påpekes at

kontroll med outsourcing krever kunnskap om hvilke verdier de eier, og betydningen av dataen. Således er det viktig å inkludere ledere på ulikt nivå ved beslutninger som omhandler outsourcing (van Scheers, 2006). Det er likevel en ulik forståelse om hva ekspertene vurderer som kritisk data, men det som utpeker seg er at ingen vektlegger *konfidensialitet, integritet* og *tilgjengelighet* i deres vurderinger. Årsaker til ulik forståelse kan komme som følge av ekspertenes forskjellige bakgrunn og kompetanse, samtidig som operatørselskapenes kultur kan påvirke hvordan ekspertene vurderer informasjonsverdier. Aktører vektlegger risikofaktorer forskjellig, noe som grunnes i at risikopersepsjon er subjektive. Således er det hensiktsmessig å være tydelig på eksperter vurderer viktigheten av faktorene forskjellig (Liu et al., 2010; Slovic, 2001). Tross at flere påpeker at de har virksomhetskritisk data, ser man at risikoen for at noe går tapt ikke oppfattes som sannsynlig. Det er imidlertid kjent at sårbarheter kan utnyttes av uautoriserte personer eller trusselaktører, noe som kan gi tilgang til organisatoriske verdier (Landoll, 2006). At ekspertene ikke vurderer informasjonen de har kan medvirkende til en større aksept av risikoen outsourcing medfører. Det kan også bidra til manglende forståelse av risiko og sårbarhet knyttet til deres verdier.

Det er bemerkelsesverdig at operatørene ikke i større grad sikrer sine verdier som følge av den økte risikoen som forekommer ved outsourcing. Enkelte eksperter vurderer derimot omdømme som en av de største risikoene, og prioriterer dette høyt i sine vurderinger. Dette kan være et sektorspesifikt fenomen, og må ses i relasjon til at informasjonssikkerhet ikke er tydelig lovfestet i sektoren. Følgelig kan dette påvirke hvordan ekspertene vurderer operatørselskapets verdier. Eksempelvis er verdier i enkelte andre sektorer hjemlet i lov, gjennom blant annet sikkerhetsloven og GDPR. Ofte er det nødvendig å vurdere sammenhenger mellom ulike faktorer (Fan et al., 2012), der det er kausalitet mellom sikring av verdier og opprettholde omdømme.

Språk og kultur

Kulturelle og språklige forskjeller kan være problematisk i forbindelse med outsourcing (Liang et al., 2015), noe ekspertene tydelig fremhever som en utfordring. Dette påvirker kvalitet på tjenestene, kommunikasjonen mellom operatør og tjenesteleverandør, samt det relasjonelle i arbeidet. Totalt går dette ut over brukervennligheten og sikkerheten. Disse utfordringene er uavhengig av hvor og om operatørene outsourcer IKT. Tidssone og avstand er faktorer som også viser seg å være av betydning for ekspertene, der lokasjon av tjenesteleverandør blir vektlagt i vurderingene. Flere eksperter mener å velge en leverandør innenlands med bransjeforståelse vil gi

bedre sikkerhet fremfor å velge leverandør i lavkostnadsland. Som kjent gjenspeiles ikke god informasjonssikkerhet bare av egen praksis, men man er avhengig av tjenesteleverandørens sikkerhetsmekanismer og praksis i tillegg (Wu et al., 2017). Det er overraskende at fagdokumenter ikke trekker frem risikoer som fremkommer av kulturelle og språklige forhold i forbindelse med outsourcing. Dette fremheves derimot av samtlige eksperter, der flere har direkte erfaring med det. Utfordringer som følge av kulturelle forhold er sektoruavhengig, og vil foreligge i de tilfeller der det velges tjenesteleverandør i lavkostland.

Tilgang og kontroll

Outsourcing av IKT-tjenester øker risikoen for at man mister kontroll over tekniske sikringstiltak og tilgang til data. Dette er spesielt problematisk i forbindelse med å opprettholde kontroll over lange og komplekse verdikjeder (NOU 2015:13; NSM, 2017a; NSM, 2017b; NSM, 2018). Derfor er det viktig med gode risikovurderinger, slik at man kan fange opp risikoer ved outsourcing (Aris et al., 2008). På bakgrunn av dette er det tankevekkende at et fåtall av ekspertene trekker frem manglende kontroll som en risiko, selv om de nevner paralleller til at outsourcing er en risiko i seg selv. Kontroll er et moment som er gjennomgående i faglitteratur og forskning på området, og således er det svært relevant for operatører som vurderer outsourcing. Dette må også ses i lys av et økende antall trusselaktører. Petroleumssektoren er stadig mer utsatt for uønskede hendelser, og en fremtredende trussel er flere angrep og innsidere (NSM, 2017a; NSM, 2017b; NUPI, 2018; PST, 2017). Forskjeller i risikoforståelsen kan være påvirket av tidligere erfaringer og holdninger, samtidig som det kan være avhengig av hvem som foretar vurderingene. Flere av ekspertene har blant annet betydelig teknisk kompetanse, som kan gjøre at flere har mer fokus på tekniske tiltak, heller enn helhetlige prosesser. Derfor er det viktig med tverrfaglighet i risikovurderinger i forbindelse med komplekse IKT-systemer, som innebærer et grensesnitt mellom ulike funksjonsområder (Fell, 2013; Tafti, 2005).

Det er interessant at manglende kontroll ikke hensyntas i vurderingene, da outsourcing krever bedre kontrollregime (Justis- og beredskapsdepartementet, 2016a). Flere eksperter fremhever derimot at det forenkler arbeidshverdagen, noe som er bemerkelsesverdig. Det er imidlertid ikke slik at en virksomhets ansvar reduseres selv om man setter ut en tjeneste, men vil faktisk føre til at de får et betydelig mer ansvar for å sikre kontroll over både informasjonsverdier og tjenesteleverandør (NSM, 2017b). Virksomhetene er ansvarlig for egen IKT-sikkerhet (Forsvarets

forskningsinstitutt, 2016), og det er et lederansvar å kontrollere risikoer ved outsourcing, inkludert håndtering og minimering av risiko (Ahmed et al., 2014). Holdningen til eget oppfølgingsansvar kan derfor utgjøre en risiko, og det er derfor interessant at få eksperter fremhever økt grad av kontroll og oppfølging ved outsourcing. Dette viser et klart behov for en holdningsendring og bedre oppfølging av leverandører for å kunne styrke sikkerheten i bransjen, noe som også er belyst av flere faginstanser (Arbeids- og sosialdepartementet, 2018; IRIS, 2018).

Det er spesiell bekymring knyttet til kontroll over tilgang til data. Det er viktig å sikre at uautoriserte personer ikke får tilgang, der et viktig tiltak er tilgangsstyring (NSM, 2017a). Flertallet av ekspertene trekker fram tilgang som en risiko, men det er få som vektlegger dette i vurderingene deres. Det er antydninger til at flere av operatørene i større grad overlater kontroll til tjenesteleverandør. Derimot er tilgangsstyring i likhet med kontroll et virksomhetsansvar, slik at de skal kunne lukke sårbarheter og øke robustheten (NSM, 2017a). Kontroll omfavner både tekniske og organisatoriske forhold, og risikovurderingene burde legge vekt på forhold som har betydning for det styrende arbeidet (Direktoratet for e-helse, 2016). De bør spesielt avdekke områder som berører kontroll og tilgang, i tillegg til at sikkerhetsmålene bør vektlegges (Dhillon et al., 2017). Hos ekspertene er vurderinger med fokus på informasjonssikkerhet mangelfulle, noe som er bemerkelsesverdig da faglitteratur innenfor IKT-sikkerhet belyser dette i utstrakt grad.

Eksperters forståelse av risiko i forbindelse med outsourcing

Ekspertene påpeker flere risikofaktorer når det kommer til outsourcing, der de mest fremtredende er kulturelle forhold og omdømme. Dette er faktorer som også vektlegges mest i vurderingene til operatørselskapene. Faktorer som verdier, tilgang og kontroll vektlegges i mindre grad, noe som er betenkelig da man ved outsourcing er prisgitt tjenesteleverandørens sikkerhetsmekanismer og praksis. Det er interessant at kausalitet mellom risikofaktorer ikke vurderes, da for eksempel uheldige hendelser som følge av manglende kontroll og tilgangsstyring kan ha direkte påvirkning på eksempelvis økonomi og sikkerhet. Tilsvarende gjelder manglende ansvarsbevissthet ved outsourcing, der enkelte virker å ta lett på tjenesteutsettingen av IKT-tjenestene. Spesielt tydelig er dette ved manglende oppfølging av tjenesteleverandør, og manglende risikovurderinger. For å forstå risikoen ved outsourcing er det derfor nødvendig med et helhetlig perspektiv som viser sammenhenger. Selv om ekspertene reflekterer over enkelte risikofaktorer, virker det ikke som risikoen forstås og anerkjennes i den grad den burde. Dersom ekspertene hadde benyttet

risikovurdering i forbindelse med outsourcing ville dette bidratt til en større forståelse av de risikoene som er fremtredende ved outsourcing av IKT-tjenester.

Flere av faktorene overfor som fremkommer er gjennomgående belyst fra flere instanser, der enkelte er mer kontekstavhengig enn andre. Spesielt når det gjelder tilgang og kontroll er det hendelser innad i sektoren, for eksempel Statoils hendelse på Mongstad som viser hvilke konsekvenser mangelfull kontroll og tilgang kan medføre. Videre kan det reflekteres over om problematikken med tilgangsstyring er et sektorspesifikt fenomen, der manglende hjemmel i lov kan legge føringer for hvordan eksperter og operatører forvalter verdiene og tilhørende sikkerhetsmekanismer.

6.2 I hvilken grad har interne og eksterne faktorer betydning for operatørers vurderinger vedrørende outsourcing?

I følgende del vil de faktorene som viser seg å ha hatt en innvirkning på hvordan eksperter vurderer outsourcing av IKT-tjenester fremheves og diskuteres. Dette inkluderer både interne og eksterne faktorer, der kapittelets oppbygging er inndelt etter hovedmomenter under henholdsvis interne og eksterne faktorer. Dette vil ses i sammenheng med hvordan eksperter vektla de risikomomenter som ble belyst i forskningsspørsmål 1.

6.2.1 Interne faktorer

Kostnad og tilgang til kompetanse

Det er anerkjent at outsourcing kan føre til fordeler knyttet til blant annet økonomi og tilgang til ressurser (Fell, 2013; Oshri et al., 2011; Gottschalk, 2005a), og kan således være en hensiktsmessig løsning for mange virksomheter (NOU 2015:13). Imidlertid er det er svært få eksperter som vektlegger kostnad, og de som gjør det outsourcer også til lavkostnadsland. Derimot er det flere eksperter som fremhever og vektlegger tilgang til ekspertise og kompetanse, som er i tråd med faglitteratur om informasjonssikkerhet på området. Dette gjør at virksomheter reduserer behovet for å bygge opp egen kompetanse selv (NOU 2015:13; NSM, 2017a). Et interessant element er at ingen eksperter trekker frem behovet for å forsterke kompetansen innad i operatørselskapet, slik at de kan etterleve nødvendig kontroll over tjenesteleverandør. Mange outsourcing-prosesser mislykkes ofte fordi de mangler denne kompetansen, samtidig som de ikke klarer å implementere

risikostyring i prosessene (Aris et al., 2008). Dette er spesielt fremtredende ved moderne komplekse og gjensidige avhengige risikoer (Aven & Renn, 2012). God bestillerkompetanse hos operatørene anses som vesentlig for å oppnå en vellykket outsourcingsprosess, og det er underlig at dette ikke trekkes frem som en risiko eller nødvendig faktor i vurderingene.

Risikovurdering

Risikovurderinger bør gjennomføres i forbindelse med outsourcing for å identifisere verdier og sårbarheter, samt for å kartlegge hvilket sikkerhetsnivå som er nødvendig (Justis- og beredskapsdepartementet, 2016b; NOU 2015:13). Det er et verktøy som danner underlag og støtte i beslutninger, der kunnskap om risiko i en gitt kontekst fremstilles og utgjør et relevant risikobilde (Aven, 2015; Aven & Guikema, 2011; Prado, 2011; Renn, 2008). Det er oppsiktsvekkende at få operatører gjennomfører fullverdige risikovurderinger. Dette på tross at viktigheten av dem understrekes, både i dokumenter og ved hendelsene som har vært i media. Risikovurderinger gjennomføres heller ikke ved nye og/eller endret tjenesteleverandør. Det er fremtredende at et fåtall har gjennomført elementer av risikovurderinger, og enkelte har vurdert risikoen som for høy. Dette samsvarer med tidligere undersøkelser som har vist at risikovurderinger ved outsourcing er mangelfulle (NOU 2015:13; NSM, 2017b; NSM 2018). Herunder kan mangelfulle eller ikke-eksisterende risikovurderinger fører til økt sårbarhet og et utilstrekkelig risikobilde, som kan medvirke til at uønskede alvorlige hendelser inntreffer (Aven, 2015).

Når det gjelder informasjonssikkerhet bør risikovurderingene inkludere ukjente og sjeldne hendelser. Slike hendelser er vanskelig å vurdere på grunnlag av sannsynlig og konsekvens alene, fordi omfanget av mulige utfall og/eller sannsynlighet er utydelige (Renn, 2007). En utfordring knyttet til IKT-sikkerhet er nettopp at problemer oppstår uventet og plutselig (Oppliger, 2015). Eksempelvis er petroleumssektoren i økende grad utsatt for risikoer som produksjonsstans, sabotasje og industrispionasje, noe Statoils outsourcingshendelse, NotPetya-viruset og Shamoon-viruset mot prosesskontrollsystemene i 2013 illustrerer (NOU 2015:13; NUPI, 2018). Det er bred enighet blant ekspertene at slike hendelser ikke kan forhindres, men det må jobbes mot å redusere konsekvensene. Sektoren er kjent for å benytte en barrieretilnærming, som det er indikasjoner på å også gjelde i forbindelse med informasjonssikkerhet. Dette ses blant annet gjennom tilgang til overvåkningstjenester av nettverk og tiltak som vil redusere omfanget av eventuelle hendelser.

Imidlertid er det få som gjennomfører trusselvurderinger, som gjør det vanskelig å forholde seg til et forverret risikobilde.

For å kunne ta gode beslutninger med hensyn til ukjente og sjeldne risikoer kan det være hensiktsmessig å benytte forsiktighetsprinsippet (Aven, 2014). Dette betyr at operatørene bør være varsomme med å outsource IKT-tjenestene ved høy usikkerhet, og eventuelt implementere tiltak som kan redusere risikoen. Dette vil imidlertid være avhengig av hvilken strategi operatørene legger til grunn i beslutningsprosessen, og hvordan ekspertene forstår og vektlegger risikoen knyttet til outsourcing. Det er derfor betinget av kunnskapen de har (Aven, 2014). Varsomhet anses formålstjenlig ved outsourcing, på bakgrunn av krav til omstillingsprosesser, et økende digitalt sårbarhetsbilde og alvorlige konsekvenser ved hendelser. Det er spesielt hensiktsmessig i en sektor med manglende IKT-kompetanse. Derimot er det svært få av operatørene som legger til grunn en forsiktighetsstrategi, der flere anser outsourcing som et tiltak for å øke IKT-sikkerheten. Både IRIS (2018) og NUPI (2018) fremhever hvordan omstillingsprosesser i forbindelse med outsourcing og digitalisering kan endre situasjonsbildet og medføre nye risikoer. Samtidig øker både trusselbildet og konsekvensenes alvorlighetsgrad (DNV GL, 2018; PST, 2017; NSM, 2017a; NSM, 2017b; NSM, 2018).

6.2.2 Eksterne faktorer

Internasjonale virksomheter

Hvordan operatørselskapene er organisert er av stor betydning for hvordan de vektlegger risiko knyttet til outsourcing, der dette er en faktor som påvirker beslutninger. Det er mange som etablerer sikkerhetssamarbeid med sine globale konsern (NOU 2015:13). Flere av operatørene opplever både krav og press fra det globale miljøet når det gjelder outsourcing og valg av tjenesteleverandør. I enkelte tilfeller var ikke outsourcing et valg, men en selvfølge. Presset det internasjonale selskapet påfører operatørene er av vesentlig betydning for deres autonomi, spesielt når det gjelder handlingsfrihet knyttet til valg og beslutninger vedrørende outsourcing. Følgelig er det av direkte betydning for hvordan og hva operatørene vektla i sine vurderinger. Ett av hovedargumentene til enkelte internasjonale operatørselskaper er standardiseringsprosesser i det globale konsernet. Tilsvarende sikkerhetsnivå på ulike kontorer vil heve sikkerhetsnivået totalt sett, og utgjør således en viktig faktor i vurderingen knyttet til outsourcing.

Risikoforståelse

Hvordan risiko og sårbarhet vektlegges avhenger av hvem som vurderer det, og konteksten det vurderes i (Aven, 2015). Sikkerhetstilstanden påvirkes av hvordan man forholder seg til risikoerkjennelse, og er viktig for å ta gode beslutninger (NSM, 2017b). Det er trukket frem at operatørene i større grad må bli bevisst på eget ansvar og hvilken kompetanse de har, slik at informasjonssikkerheten ivaretas. Det er indikasjoner på svak risikoforståelse hos ekspertene i forbindelse med outsourcing, som dels kan komme på bakgrunn av manglende risikovurderinger. Dette er også en utfordring som trekkes frem av fagmiljøene, der virksomheter mener egen sikkerhetstilstand er god, tross manglende dokumentasjon for å fremsette det (NSM, 2017b).

Interne og eksterne faktorers betydning for risikovurderinger

Det er flere faktorer som har innvirkning på ekspertenes vurdering vedrørende outsourcing. Når det gjelder tilgang på kompetanse og fokus på kjernevirksomhet er dette interne faktorer som er av betydning for ekspertenes valg i henhold til outsourcing. Imidlertid har ikke faktorenes risiko samme betydning for ekspertenes vurdering. Når det kommer til eksterne faktorer er press fra det internasjonale miljøet av stor betydning for valg og vurdering i relasjon til outsourcing. Videre er risikoforståelse, risikovurdering og GDPR faktorer som påvirker valg som tas. Derimot er det flere underliggende faktorer som virker å bety mer i vurderingene enn de eksplisitte risikoene som trekkes frem. Resultatene belyses mye i tidligere forskning vedrørende outsourcing, bortsett fra betydningen det globale konsernet har. Dette fremstår sektorspesifikt. Det kan også diskuteres hvorvidt deres føringer på valg og beslutninger med tanke på outsourcing er mulig på grunn av svakt regelverk og styring på området.

Manglende risikovurderinger fører til manglende risikoforståelse, som gjør at operatører ikke har korrekt risikobilde. Med tanke på hvor ofte dette er belyst i faglitteratur og media, er det oppsiktsvekkende at operatørene ikke gjennomfører risikovurderinger. Resultater fra NSM (2017a; 2017b; 2018) viser at dette er gjennomgående, og således ikke avvikende fra andre sektorer eller områder. Det kan reflekteres over årsaken til at risikovurderinger ikke gjennomføres i større grad, der dette gjerne begrunnes i to elementer; kompetanse og/eller tid og ressurser. I operatørselskapene legges det imidlertid til rette å gjennomføre risikovurderinger, der det allokeres tilstrekkelig med ressurser. Dermed kan det stilles spørsmål ved om operatørene har nødvendig og korrekt kompetanse for å gjennomføre risikovurderinger. I petroleumssektoren kan årsaken være

manglende sikkerhetskompetanse innen IKT, noe som kan forklare hvorfor risikovurderinger er utilstrekkelig. Dette viser at operatører ikke ser sitt oppfølgingsansvar når det kommer til IKT-sikkerhet, herunder oppfølging av tjenesteleverandør og sikker bestillerkompetanse. Generelle slutninger som fremkommer er at eksterne faktorer er av større betydning enn interne. Enkelte av faktorene som er av størst betydning kan ikke påvirkes av ekspertene. Det understrekes at flertallet av ekspertene som outsourcer IKT-tjenester ville valgt annerledes når det kommer til outsourcingsmodell og/eller tjenesteleverandør.

6.3 Hvordan påvirker læring og styring i sektoren operatørers vurderinger når det gjelder informasjonssikkerhet?

For å få en helhetsforståelse av operatører vurderinger knyttet til outsourcing av IKT-tjenester er det valgt å inkludere læring og styring i sektoren. Delkapittelet er strukturert etter henholdsvis læring og styring. Dette er inkludert da de er del av operatørers eksterne kontekst, og følgelig kan ha innvirkning på eksperters risikoforståelse og vurderinger ved outsourcing. I tillegg setter styring i sektoren rammer for operatører. Det anses formålstjenlig å inkludere sektoren, da flere av utfordringene knyttet til outsourcing er sektorspesifikke problemstillinger.

6.3.1 Læring

Læring i egen virksomhet

Læring i egen virksomhet kan bidra til å oppdage nye sårbarheter eller forbedringspunkter, og kan hindre at hendelser oppstår (NSM, 2017a). Erfaring kan inntreffe ved vanlige og uvanlige hendelser, og kan bidra til innblikk i deres forutsetninger for å håndtere det uforutsette (Engen et al., 2016; Lampel et al., 2009). Operatørene fremstår som god på intern læring, spesielt med tanke på brukerbevissthet. Flere av ekspertene påpeker viktigheten med å ha kampanjer om informasjonssikkerhet, og trekker samtidig paralleller til brukervennlighet på systemene. En generell oppfatning er at bevisstheten er høy med tanke på virus og svindelforsøk. På dette området viser operatørene at de jobber godt med sikkerhetsbarrierer, forbedring av ytelse og vedlikehold. Dette er egenskaper som gjenkjennes i resiliente organisasjoner, som også karakteriseres ved at de er forberedt på endring, variasjon og forstyrrelser (Aven, 2014). Læring kan forbedre eksisterende prosesser, og danne en forståelse for risiko i vurderinger vedrørende outsourcing.

Læring av hendelser mellom virksomheter

Det er stor avhengighet og kontraktuelle forhold mellom virksomheter i petroleumsbransjen, noe som medfører økt behov for samhandling mellom aktører (IRIS, 2018; NOU 2015:13). Det er viktig å dra læring av tidligere hendelser (NSM, 2017a), noe som er et vesentlig moment i forbindelse med outsourcing. Særlig gjelder dette for å bli mer robuste mot samtidens utfordringer og trusler. Virksomheter bør kommunisere og dele deres erfaringer rundt hendelser som inntreffer, og har et ansvar for hvordan egne handlinger kan påvirke andre (Justis- og beredskapsdepartementet, 2016a; Justis- og beredskapsdepartementet, 2016b). Det er bemerkelsesverdig at operatørene er restriktive med å dele informasjon, spesielt sett i lys av at sikkerhetsrelatert informasjon er noe som er nyttig for samtlige. Overføring av kunnskap og informasjon kan føre til en felles utvikling (Wenger, 1998), og således føre til at virksomheter blir bedre rustet til å håndtere risiko og sårbarhet. Paradokset er at operatørene ønsker å motta informasjon, men ikke dele. Den restriktive holdningen til å dele informasjon beror på omdømme, som prioriteres høyt. Generelle slutninger vedrørende læring i operatørenes vurderinger vektlegges lite. I en sektor med kompleks infrastruktur, der aktører er avhengige av hverandre (NOU 2015:13), er det interessant at det ikke legges opp til mer samordnet læring for å kunne forhindre og håndtere uønskede hendelser. Hendelsen i Maersk fremhever viktigheten med dele informasjon, der aktører er sammenkoblet og hendelser skaper ringvirkninger.

Læring mellom virksomheter og eksterne aktører

Et moment som trekkes frem er utfordring med informasjonsdeling mellom virksomheter og eksterne aktører (NUPI, 2018). Fageksperter belyser at mindre virksomheter uten internasjonalt apparat har større behov for tydelige retningslinjer vedrørende IKT-sikkerhet, noe som samsvarer med det flere eksperter har trukket fram. Det stilles særlig spørsmålstegn ved hvor mye Ptil skal involvere seg ved å etablere en felles arena for læring, da det i hovedsak er et behov hos små virksomheter. Det påpekes at alvorlighetsgraden ved hendelser varierer, der store selskap gjerne påføres større konsekvenser, som også kan gå ut over samfunnet generelt sett. Selv om små operatørselskap kan påføre små konsekvenser, vil den gjensidige avhengigheten øke sannsynligheten og risikoen for at små hendelser også kan medføre store konsekvenser. Risikoforståelsen vedrørende outsourcing beror på kunnskapsgrunnlaget ekspertene har (Liu et al., 2010), og ulike faktorer vektlegges forskjellig blant ulike aktører (Prado, 2011). En felles arena

gjennom direktorat og tilsyn kan gi stort læringsutbytte for virksomhetene med hensyn til kunnskapsdeling, der informasjon deles mellom ulike deltakere (SINTEF, 2011; Kvale & Nielsen, 1999).

6.3.2 Styring

Risikostyring

De årlige vurderingene gjennomført av blant annet NSM kan være et viktig bidrag i virksomheters risikostyring, i tillegg til at det kan skape bedre risikoforståelse (Justis- og beredskapsdepartementet, 2016b). Effektiv hendelseshåndtering og risikostyring har stort sett vært mangelvare når det gjelder informasjonssystemer. Dette bør forbedres, og bør integreres i virksomheters overordnet styring (NSM, 2017b). Blant annet kan dette gjøres gjennom revisjoner, samarbeid og kunnskapsdeling i sektoren (IRIS, 2018). Styring fra sektoren innebærer blant annet å definere rammebetingelser for virksomheter. Dette legger også føringer for handlingsmulighet (Rasmussen, 1997). Fordi risikostyring blant annet innebærer kommunikasjon og håndtering av beslutninger (Aven & Renn, 2012), kan man trekke slutninger ved hvor gode risikostyringsprosesser knyttet til outsourcing av IKT-tjenester er i petroleumssektoren. Dette må ses i sammenheng med læring og samhandling, da summen av faktorene gir et bilde av risikostyringsprosessene. Det betviles ikke at operatørene har fokus på risiko knyttet til outsourcing, men det stilles spørsmål ved om prosessen er tilstrekkelig.

Tilsyn

Det har blitt gjennomført lette tilsyn fra Ptil når det gjelder informasjonssikkerhet de siste årene, der enkelte mener det er usikkerhet rundt hensikten og mener det er mer en statusoppdatering. Det er tidligere påpekt at Ptil har behov for mer teknisk kompetanse, og at det bør etableres felles retningslinjer og standarder i bransjen (NOU 2015:13; IRIS, 2018). En av hovedutfordringene til Ptil er at de ikke har lovverk som setter klare rammer, og dermed er det vanskelig å føre tilsyn. Det er konflikterende meninger rundt hvorvidt lovverket bør styrkes. Mens enkelte operatører og Ptil er kritisk til et mer spesifikt og styrende regelverk, er det andre operatører og fagdokumenter som påpeker et større behov for dette grunnet utviklingen i sektoren. Beslutningstakere og eksperters vurderinger vil være avhengig av aktiviteter fra andre og faktorer i omgivelsene (Rasmussen, 1997). I relasjon til informasjonssikkerhet har tilsynet stor påvirkningskraft overfor

de valg og forhold som virksomheter bør vektlegges. På den måten kan Ptil bidra til å forhindre målkonflikter (SINTEF, 2009).

Det er tidligere kommet frem at Ptil virker passive når det gjelder å tilpasse seg digitalisering i sektoren (IRIS, 2018), noe som samsvarer med våre analyser. Ptil fremhever et klart skille mellom OT og IT, der det pekes på at deres ansvarsområde er på OT-siden. Imidlertid er det flere som viser til større integrasjon på hele den digitale plattformen (IRIS, 2018; Røsjø, 2009). Statoils nylansering på EnergyWorld 2018 viser dette der de satser på en helhetlig skyløsning, basert på Microsofts Azures teknologi. Det er dermed på tide å diskutere hvilken rolle ulike instanser og myndigheter skal ha fremover. Spesielt fordi behovet for gode IKT-løsninger ikke vil reduseres i tiden fremover, og som kan innebære økt behov for outsourcing.

Helhetlig tilnærming

Informasjonssikkerhet krever et etablert styringssystem (Justis- og beredskapsdepartementet, 2016a), for å kunne redusere digitale sårbarheter. Disse kan baseres på anerkjente standarder, slik at gode sikringstiltak ses opp mot virksomhetens overordnede styringsprosess (NSM, 2017b). Metoder for risikostyring i sektoren har ikke utviklet seg i takt med digitaliseringen. Derfor stilles det spørsmål ved om det eksisterende rammeverket, med metoder og prinsipper for risikostyring, er godt nok (IRS, 2018). Det bør stilles krav til virksomheter om beskyttelse av verdier, der departementet bør tydeliggjøre krav og føringer i forbindelse med dette (NOU 2015:13). Imidlertid er det noe tvetydighet sett mot hvordan operatører og Petroleumstilsynet oppfatter dette. Interessant her er at enkelte mener beste praksis fra tjenesteleverandører er tilstrekkelig, dog er man da prisgitt outsourcing. Derimot ser man at enkelte trekker fram at GDPR er direkte betydning for tjenestemodell og/eller valg av tjenesteleverandør.

Hvordan læring og styring påvirker outsourcing i sektoren

Overordnede konklusjoner som kan sammenfattes fra læring i sektoren er at operatørene er god på læring internt. Derimot er operatører mindre gode på læring seg i mellom, noe som kan reflekteres i risikoforståelsen. Samtidig vil kunnskapsdeling bedre deres evne til å foreta velinformerte vurderinger og beslutninger knyttet til outsourcing. Videre viser det seg at lover og forskrifter knyttet til informasjonssikkerhet vil gi økt mulighet for sikker håndtering av risiko. Det

fremkommer at styring vil påvirke de valg og beslutninger operatører tar, men at det er tvetydighet knyttet til om det er tilsynet sin rolle.

Læring påvirker ikke operatører vurderinger i stor grad, men kunne gjort det med bedre samhandling og kunnskapsdeling i sektoren. Dette ville lagt grunnlag for velinformerte beslutninger basert på oppdatert kunnskap om trusselbildet. Det faktum at det er lite styring i sektoren gir operatørene stor handlingsfrihet, og er følgelig av stor betydning for de valg som tas. Derimot ville styring vært av stor betydning dersom det hadde vært tydeligere rammer, og bedre risikostyring i sektoren i forbindelse med IKT. Generelt kan det trekkes konklusjoner dit hen at utfordringene som samfunnet står over krever god risikostyring på virksomhetsnivå, men også sektornivå der tilsyn og myndigheter er sentrale aktører.

Framtidens trusselbilde, økt digitalisering og gode løsninger for IKT-systemer er noe som øker risikoen for uheldige hendelser. Dette påpekes til stadighet i fagdokumenter og debatter, og er et sektorovergripende problem. Samtidig påpekes det at operatørene er selv ansvarlige for egen IKT-sikkerhet. Det er tankevekkende at hendelser innen IKT gjerne påvirker flere enn operatøren selv, noe det økte antallet angrep på underleverandørnivå viser. Da petroleumssektoren er en viktig samfunnsfunksjon, med komplekse og gjensidige avhengigheter, er det viktig å forebygge og forberede seg på digitale hendelser. For at operatørene skal kunne holde tritt med utviklingen av ny teknologi, større integrasjon mellom nett og samtidig beskytte sine verdier som følge av et endret risikobilde er det nødvendig med økt fokus på risikostyring ved outsourcing. Spesielt gjelder dette med tanke på det ukjente og usikkerheten det åpner opp for. Med hensyn til dette er IKT-sikkerhet et område som er forholdsvis nytt og i stadig utvikling. Det er økt behov for utvikling av gode praksiser og retningslinjer når det gjelder informasjonssikkerhet, så vel som det gir et økt behov for videre forskning på området. Spesielt fremtredende er anvendelsen av risikovurderinger, samt forståelsen av det komplekse samspillet rundt samtidens utfordringer. Dette er områder som er aktuelle for videre forskning i samtlige sektorer.

7. Konklusjon

Studien har bidratt med å belyse hvordan operatører på norsk sokkel benytter risikovurderinger når det gjelder outsourcing av IKT, og hvilke faktorer i omgivelsene som påvirker deres vurderinger. Flere aspekter som er belyst viser seg å være sektoruavhengig, og er således utfordringer som krever tverrsektoriell samhandling. Problemstillingen har vært som følger;

«*På hvilken måte benytter operatører risikovurderinger i forbindelse med outsourcing av informasjons- og kommunikasjonsteknologi, og hvilke forhold påvirker ekspertenes vurderinger?*»

Outsourcing av IKT-tjenester er et økende fenomen, og benyttes i utstrakt grad i samtlige sektorer og virksomheter. Petroleumssektorens digitaliseringsprosess har økt behovet for gode IKT-løsninger, der outsourcing bidrar til kompetanse, effektivitet og kostnadsreduksjon. Imidlertid øker outsourcing av IKT-tjenester risikoen for uønskede hendelser, som følge av et stadig forverret trusselbilde og lengre verdikjeder. For å ivareta informasjonssikkerhet ved tjenesteutsetting kreves det bedre kontroll og styring, fortrinnsvis gjennom en risikobasert tilnærming. Operatørene benytter risikovurderinger i varierende grad, der de fleste ikke har gjennomført fullverdige risikovurdering med tilhørende analyser. Faktorer og forhold i omgivelsene påvirker operatørenes valg og vurderinger når det gjelder beslutninger om outsourcing, der fordeler vektlegges fremfor risikoer.

Ekspertenes risikoforståelse begrenses til enkeltfaktorer, heller enn helhetsforståelse, og resulterer i et snevert risikobilde. Omdømme prioriteres høyt i operatørenes vurderinger, der flere av valgene og vurderingene sentreres rundt dette. Risikofaktorer anerkjennes derimot ikke tilstrekkelig, spesielt med tanke på kausalitet, kompleksitet og gjensidig avhengighet. Interne faktorer av størst betydning for eksperters risikoforståelse er manglende risikovurderinger og eierskap til egne verdier. I tillegg er svak risikostyring fra sektoren og fragmentert regelverk i forbindelse med IKT-sikkerhet eksterne faktorer med sterk påvirkning vedrørende hvordan operatører forholder seg til outsourcing av IKT-tjenester. Det reflekteres over om dette er sektorspesifikke karakteristikker. Sett i lys av andre sektorer, herunder helse, kraft og finans, er forvaltning og informasjonssikkerhet vedrørende verdiene hjemlet i lov. Dette begrunnes med at verdiene andre sektorer forvalter er av

stor samfunnsmessig betydning. Imidlertid kan det diskuteres hvorvidt petroleumssektorens verdier og samfunnsfunksjon også bør inkorporeres i regelverk som i større grad ivaretar informasjonssikkerheten.

Petroleumssektoren har sterk påvirkning fra omgivelsene, gjennom tilsyn og internasjonale selskap. Sistnevnte påvirker operatørers autonomi, og legger sterke føringer for valg og beslutninger vedrørende outsourcing, der det for enkelte ikke er en vurdering, men en selvfølge. Læring i sektoren har svak innvirkning i vurderingene, og det er behov for større erfarings- og kunnskapsoverføring som kan bidra til å forbedre prosesser rundt outsourcing. Myndighetenes rolle av betydning for eksperters risikoforståelse, og operatørers valg når det kommer til outsourcing. Spesielt fordi manglende styring og hjemmel i lov gir operatører stort handlingsrom, har dette innvirkning på hvordan operatørene forholder seg til risiko. Fokusområdene til Ptil er direkte overførbare til operatørers fokusområder, noe som viser at det er klar sammenheng mellom myndigheter og operatører.

Flere av forholdene i studien er sektoruavhengig. Dette bygger opp under at mange av utfordringene i forbindelse med outsourcing er tverrsektorielle, der gode løsninger fortsatt er mangelvare. Dette tydeliggjør behov for kommunikasjon og samhandling mellom både virksomheter, sektorer og myndigheter, der man i fellesskap kan utvikle robuste systemer og risikostyringsprosesser. Det kan med fordel legges til grunn en tydeligere risikobasert tilnærming når det gjelder informasjonssikkerhet, der spesielt myndigheter og tilsyn bør ta en mer fremtredende rolle. IKT er et område i stadig utvikling, og det krever at bransjen klarer å tilpasse seg deretter. Det krever bevissthet, fokus og holdningsendring. Imidlertid er IKT-sikkerhet en kontinuerlig prosess, og et område som må styrkes.

8. Litteraturliste

Andersen, S.S. (2006). Aktiv informantintervjuing. *Norsk statsvitenskapelig tidsskrift,* Vol. 22, pp. 278-298. Hentet fra: https://www-idunn.no.ezproxy.uis.no/nst/2006/03/aktiv_informantintervjuing

Akhgar, B. og Hamid, R. A. (2014). *Emerging trends in ICT security*. Hentet fra: https://ebookcentralproquestcom.ezproxy.uis.no/lib/uisbib/reader.action?docID=1562332&query

Arbeids- og sosialdepartementet. (2018). *Helse, miljø og sikkerhet i petroleumsvirksomheten.* (Meld. St. 12 2017-2018). Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-12-20172018/id2595598/

Aris, S.R.H.S., Arshad, N.H. & Mohamed, A. (2008). Conceptual framework on Risk Management in IT outsourcing projects. *WSEAS Transactions on information science & applications, Vol. 5*(4), pp. 816-831. ISSN: 1790-0832

Aven, T. (2007). *Risikostyring.* Oslo: Universitetsforlaget.

Aven, T. (2010). *Misconceptions of risk.* United Kingdom: John Wiley & Sons Ltd.

Aven, T. (2014). *Risk, surprises and black swans. Fundamental ideas and concepts in risk assessments and risk management*. New York: Routledge.

Aven, T. (2015c). Implications of black swans to the foundations and practice of risk assessment and management. *Reliability Engineering and System Safety, Vol. 134,* pp. 83–91. https://doi.org/10.1016/j.ress.2014.10.004

Aven, T. (2015a). *Risikostyring.* (2.utg.). Oslo: Universitetsforlaget.

Aven, T. (2015b). *Risk Analysis.* Chichester: John Wiley & Sons.

Aven, T., Boyesen, M., Njå, O., Olsen, K.H. & Sandve, K. (2004). *Samfunnssikkerhet.* Oslo: Universitetsforlaget.

Aven, T. & Guikema, S. (2011). Whose uncertainty assessments (probability distributions) does a risk assessment report: the analysts' or the experts'?. *Reliability Engineering and System Safety 96, Vol 96,* pp. 1257–1262. https://doi.org/10.1016/j.ress.2011.05.001

Aven, T. & Renn, O. (2012). On the Risk Management and Risk Governance of Petroleum Operations in the Barents Sea Area. *Risk Analysis, Vol. 32*, Nr. 9, pp. 1561 - 1575. DOI: 10.1111/j.1539-6924.2011.01777.x

Aven, T., Røed, W. & Wiencke, H.S. (2008). *Risikoanalyse. Prinsipper og metoder, med anvendelser.* Oslo: Universitetsforlaget.

Bachlechner, D., Thalmann, S. & Maier, R. (2013). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. *Computers & Security,* Vol 40, pp. 38-59. https://doi.org/10.1016/j.cose.2013.11.002

Bahli, B. & Rivard, S. (2003). The information technology outsourcing risk: a transaction cost and agency theory-based perspective. *Journal of Information Technology,* Vol. 18, pp. 211–221. DOI: 10.1080/0268396032000130214

Betten, T. & Pettersen, K. V. (2015). *Samfunnssikkerhet og beredskap - læring og endring i kommunal sektor.* Trondheim: Norges teknisk-naturvitenskapelige universitet.

Blaikie, N. (2010). *Designing Social Research* (2. utg.). Cambridge: Polity Press.

Cezar, A., Cavusoglu, H. & Raghunathan, S. (2014). Outsourcing information security: Contracting issues and security implications. *Management Science, Vol. 60*(3), pp. 638-657. https://doi-org.ezproxy.uis.no/10.1287/mnsc.2013.1763

Chirgwin, R. (2018). *IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation bliz.* Hentet fra: https://www.theregister.co.uk/2018/01/25/after_notpetya_maersk_replaced_everything/

Dalin, Å. (1999). *Veier til den lærende organisasjon*. Oslo: Cappelen Damm Akademisk Forlag.

Danermark, B. (1997). Generalisering, vetenskapeliga slutledningar och modeller för förklarande samhallsvetenskap. I Danemark, B. (1997). *Att förklara samhället.* Lund: Studentlitteratur.

Dhillon, G., Syedb, R. & de Sá-Soaresc, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management, Vol 54,* pp. 452–464. DOI: 10.1016/j.im.2016.10.002

Direktoratet for e-helse. (2016). *Norm for informasjonssikkerhet.* (5.utg., versjon 5.2). Hentet fra: https://ehelse.no/Documents/Normen/2%20Normen%20prosessdok/Norm%20for%20informasjonssikkerhet.pdf

DNV GL. (2015). *Digitale sårbarheter Olje & Gass.* (Rapport 2015-0462). Hentet fra: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/5.pdf

DNV GL. (2018). *THE STATE OF SAFETY. The outlook for the oil and gas industry in 2018.* Hentet fra: http://images.e.dnvgl.com/Web/DNVGL/%7B521cc7c2-dcbb-4f44-b5f5-33d3aae18fd1%7D_DNV_GL_-_Safety_Whitepaper_2018-Digital-Spreads.pdf

Doomun, M.R. (2008). Multi-level information system security in outsourcing domain. *Business Process Management Journal, Vol. 14* (6), pp.849-857. DOI: 10.1108/14637150810916026

eForvaltningsforskriften. (2004). Forskrift om elektronisk kommunikasjon med og i forvaltningen m.v av 01 juli 2004. Hentet fra: https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

Ekroll, H.C., Bjerkan, L. & Olsen, T. (2017). Nødnett-direktorat: Kan ikke svare på hvor lenge indiske arbeidere har hatt lovstridig tilgang til kritisk kommunikasjonssystem. *Aftenposten.* Hentet fra: https://www.aftenposten.no/norge/i/06512/Nodnett-direktorat-Kan-ikke-svare-pa-hvor-lenge-indiske-arbeidere-har-hatt-lovstridig-tilgang-til-kritisk-kommunikasjonssystem

Elvevold, E.B. (2018). Hackerangrep i Norge kan ta strupetak på kalde briter. *E24.* Hentet fra: https://e24.no/energi/storbritannia/hackerangrep-i-norge-kan-ta-strupetak-paa-kalde-briter/24272793

Engen, O.A.H., Kruke, B.I., Lindøe, P.H., Olsen, K.H., Olsen, O.E. & Pettersen, K.A. (2016). *Perspektiver på samfunnssikkerhet.* Oslo: Cappelen Damm Akademisk.

Fan, Z-P., Suo, W-L. & Feng, B. (2012). Identifying risk factors of IT outsourcing using interdependent information: An extended DEMATEL method. *Expert systems with Applications, Vol. 39*(3), pp. 3832-3840. DOI: 10.1016/j.eswa.2011.09.092

Fell, G.J. (2013). *Decoding the IT Value Problem: An Executive Guide for Achieving Optimal ROI on Critical IT Investments.* John Wiley & Sons, Incorporated.

Feng, N., Wang, H. & Li, M. (2014). A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Information sciences, Vol. 256,* pp. 57-53. DOI: 10.1016/j.ins.2013.02.036

Forsvarets forskningsinstitutt. (2016). *Vurdering av forebyggende sikkerhet innen kraft, petroleum og luftfart – sluttrapport til Sikkerhetsutvalget.* (FFI-rapport 16/00702).

Fribo, A. (2017). Dansk CEO i skarp kritik af cybersikkerheden hos Mærsk: Mærsk kan simpelthen ikke have haft et særligt højt niveau af cybersikkerhed. *Computerworld*.

Hentet fra: https://www.computerworld.dk/art/240498/dansk-ceo-i-skarp-kritik-af-cybersikkerheden-hos-maersk-maersk-kan-simpelthen-ikke-have-haft-et-saerligt-hoejt-niveau-af-cybersikkerhed

Frost, C. (2000). Outsourcing or increasing risks? *Emerald Insight*, Vol. 8(2), pp.34-37 https://doi.org/10.1108/09657960010338599

Goodman, S. E. & Ramer, R. (2007). Identifying and Mitigate the Risks of Global IT Outsourcing. *Journal of Global Information Technology Management, Vol.10(4)*, pp.1-6. DOI: 10.1080/1097198X.2007.10856452

Gottschalk, P. (2005a). *Outsourcingledelse.* Oslo: Cappelen Akademiske forlag.

Gottschalk, P. (2005b). *Sourcing av IT-tjenester. Lokalisering, organisering og styring av IT-funksjoner.* Kristiansand: Høyskoleforlaget.

Gottschalk, P. (2013). *Flytting av arbeidsoppgaver til utlandet.* Hentet fra: https://www.finansforbundet.no/wp-content/uploads/2017/01/Flytting-av-oppgaver-til-utlandet.pdf

Grønli, K.S. (2012). *Når plattformen krasjer.* Hentet fra: https://forskning.no/olje-og-gass-sikkerhet-bransje-ikt-bransje-petroleum/2012/10/nar-plattformen-krasjer

Grønmo, S. (2004). *Samfunnsvitenskapelig metoder.* Bergen: Fagbokforlaget.

Hotvedt, S. K. og Røset, H. H. (2017). Dette har skjedd i den svenske IT-skandalen. *NRK.* Hentet fra: https://www.nrk.no/urix/dette-er-den-svenske-it-skandalen-1.13614666

IRIS. (2018). *Digitalisering i petroleumsnæringen. Utviklingstrender, kunnskap og forslag til tiltak.* (Rapport - 2018/001).

ISA. (u.å). *ISA99, Industrial Automation and Control Systems Security*. Hentet fra: https://www.isa.org/isa99/

Jacobsen, F. (2017). Sikkerhet på anbud. *VG.* Hentet fra: https://www.vg.no/nyheter/meninger/i/zqj51/sikkerhet-paa-anbud

Jacobsen, D. I., & Thorsvik, J. (2007). *Hvordan organisasjoner fungerer*. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Johannessen, A., Christoffersen, L. & Tufte, P. A. (2011). *Forskningsmetode for økonomisk-administrative fag.* (3. utg.). Oslo: Abstrakt forlag.

Justis- og beredskapsdepartementet. (2016a). *IKT-Sikkerhet - Et felles ansvar.* (Meld. St. 38 2016-2017). Hentet fra:

https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

Justis- og beredskapsdepartementet. (2016b). *Risiko i et trygt samfunn - samfunnssikkerhet.* (Meld. St. 10 2016-2017). Hentet fra: https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/

Jørgenrud, M. (2017a). *Mærsk tapte opptil 2,5 milliarder kroner på dataangrep.* Hentet fra: https://www.digi.no/artikler/maersk-tapte-opptil-2-5-milliarder-kroner-pa-dataangrep/411585

Jørgenrud, M. (2017b). *Økt skepsis til IT-outsourcing i Norge. Se hvilke leverandører kundene liker best og dårligst.* Hentet fra: https://www.digi.no/artikler/okt-skepsis-til-it-outsourcing-i-norge-se-hvilke-leverandorer-kundene-liker-best-og-darligst/379845

Khalfan, A.M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management, 24,* pp. 29–42. DOI: 10.1016/j.ijinfomgt.2003.12.001

Kim, J. Y., Kim, A.S. & Miner, A. S. (2009). Organizational learning from extreme performance experience - the impact of success and recovery experience. *Organization Science, Vol 20* (6), pp. 958 - 978. https://doi.org/10.1287/orsc.1090.0439

Kommunal- og moderniseringsdepartementet. (2015). *Digital agenda for Norge - IKT for en enklere hverdag og økt produktivitet.* (Meld. St. 27 2015-2016). Hentet fra: https://www.regjeringen.no/contentassets/fe3e34b866034b82b9c623c5cec39823/no/pdfs/stm201520160027000dddpdfs.pdf

KonKraft. (2018). Konkurransekraft – norsk sokkel i endring. Hentet fra: http://konkraft.no/wp-content/uploads/2018/02/Konkurransekraft-_fullstendig_rapport_web_ny-06.03.18.pdf

Kvale, S. & Brinkmann, S. (2009). *Det kvalitative forskningsintervju.* (2.utg.). Oslo: Gyldendal Norsk forlag AS.

Kvale, S. & Nielsen, K. (1999). *Mesterlære: læring som sosial praksis.* Oslo: Ad Notam Gyldendal

Lacity, M.C., Khan, S.A. & Willcocks, L.P. (2010). A review of the IT outsourcing empirical literature and future research directions. *Journal of information technology,* Vol 25(4), pp. 395-433. Hentet fra: https://link.springer.com/article/10.1057/jit.2010.21

Lampel, J., Shamsie, J. & Shapira, Z. (2009). Experiencing the improbable- Rare events and organizational learning. *Organizational Science, Vol. 20,* pp. 835- 845. Hentet fra: http://pubsonline.informs.org/doi/abs/10.1287/orsc.1090.049

Landoll, D.J. (2006). *The security risk assessment handbook. A complete guide for performing security risk assessments.* New York: Auerbach Publications. Taylor & Francis Group.

Lee, C.K.M., Yeung, C. & Hong, Z. (2012). An integrated framework for outsourcing risk management. *Industrial Management & Data Systems,* Vol. 112(4), pp. 541-558. DOI: 10.1108/02635571211225477

Liang, H., Wang, J-J., Xue, Y. & Cui, X. (2016). IT outsourcing research from 1992 to 2013: A literature review based on main path analysis. *Information management,* Vol. 53, pp. 227-251. DOI: 10.1016/j.im.2015.10.001

Liu, S., Zhang, J., Keil, M. & Chen, T. (2010). Comparing senior executive and project manager perceptions of IT project risk: a Chinese Delphi study. *Information Systems Journal, Vol.20(4)*, pp. 319-355. DOI: 10.1111/j.1365-2575.2009.00333.x

Lofstedt, R. E. (2003). The precautionary principle: Risk, regulation and Politics. *Trans IChemsE, Vol. 81*, pp. 36-43. DOI: 10.1205/095758203762851976

Loukis, E. & Kyriakou, N. (2018). *Contractual and Relational Governance, ICT Skills and Organization Adaptations, and Cloud Computing Benefits*. Hentet fra: https://scholarspace.manoa.hawaii.edu/bitstream/10125/50480/1/paper0593.pdf

Lunnan, R. & Lervik, J. E.B. (2015). Kompetanse for å lykkes med outsourcing og offshoring. *BI forskning: Outsourcing og offshoring.* Hentet fra: https://www.bi.no/forskning/business-review/articles/2015/02/hva-du-ma-vite-for--a-flytte-ut-aktiviteter/

Majdán, G. (2012). *Governance Models in Offshore IT Outsourcing. Collaboration in Outsourcing: A Journey to Quality.* New York, NY: Palgrave Macmillan.

Nassimbeni, G., Sartor, M. & Dus, D. (2012). Security risks in service offshoring and outsourcing. *Industrial Management & Data Systems,* Vol. 112(3), pp. 405-440. DOI: 10.1108/02635571211210059

Niazi, M., Ikram, N., Bano, M., Imtiaz, S. & Khan, S.U. (2013). Establishing trust in offshore software outsourcing relationships: an exploratory study using a systematic literature review. *IET Software,* Vol. 7(5), pp. 283-293. DOI: 10.1049/iet-sen.2012.0136

Njå, O., Solberg, Ø. & Braut, G.S. (2017). Uncertainty - it´s ontological status and relation to safety. In Motet, G. & Bieder, C. (red.), *The illusion of risk control: What would it take to live with uncertainty?* Cham: Springer.

Norsk olje og gass. (2009A). *110 - Norwegian oil and gas recommended guidelines for implementation of information security in process control, safety and support ICT systems during the engineering, procurement and commissioning phases.* Hentet fra: https://www.norskoljeoggass.no/Global/Retningslinjer/Integrerte%20operasjoner/110%20%20Recommended%20guidelines%20for%20implementation%20of%20information%20security.pdf

Norsk olje og gass. (2009B). *123 - Norwegian Oil and Gas Association Guideline for Classification of process control, safety and support ICT systems based on criticality.* Hentet fra: https://www.norskoljeoggass.no/Global/Retningslinjer/Integrerte%20operasjoner/123%20%20Recommended%20guidelines%20for%20classification%20of%20process%20control%20safety%20and%20support.pdf

Norsk olje og gass. (2016). *104 – Norwegian Oil and Gas recommended guidelines on information security baseline requirements for process control, safety and support ICT systems.* Hentet fra: https://www.norskoljeoggass.no/Global/Retningslinjer/Integrerte%20operasjoner/104%20%20recommended%20guidelines%20on%20security%20baseline%20requirements.pdf

Norwegian Institute of International Affairs. (2018). Cyber-weapons in International Politics: Possible sabotage against the Norwegian petroleum sector. (NUPI report 3/2018). Hentet fra: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2486814/NUPI_Report_2018-3.pdf?sequence=1&isAllowed=y

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Hentet fra: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2016:19. (2016). *Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.* Hentet fra: https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/

NSM. (2017a). *Helhetlig IKT-risikobilde 2017*. Oslo: Nasjonal sikkerhetsmyndighet. https://nsm.stat.no/globalassets/rapporter/helhetlig_ikt-risikobilde_2017_orig_enkeltsider_low.pdf

NSM. (2017b). *Risiko 2017*. Oslo: Nasjonal sikkerhetsmyndighet. Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2017_lr_0404_enkelts_v3.pdf

NVE. (2017). *Informasjonssikkerhetstilstanden i energiforsyningen*. (Rapport nr. 90-2017). Oslo: Norges vassdrag og energidirektorat. Hentet fra: http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf

Næringslivets sikkerhetsråd. (2016). *Mørketallsundersøkelser 2016. - Informasjonssikkerhet, personvern og datakriminalitet.* (NSR-rapport 2016). Hentet fra: https://www.nsr-org.no/getfile.php/Bilder/Mørketallsundersøkelsen/morketallsundersokelsen_2016.pdf

Oppliger, R. (2015). Quantitative Risk Analysis in Information Security Management: A Modern Fairy Tale. *IEEE Security & Privacy, Vol.13(6)*, pp.18-21. DOI: 10.1109/MSP.2015.118

Oshri, I., Kotlarsky, J., & Willcocks, L. P. (2011). *The handbook of global outsourcing and offshoring*. Palgrave Macmillan.

Petroleumsloven. (1996). Lov om petroleumsvirksomhet av 29. november 1996 nr. 43. Hentet fra: https://lovdata.no/dokument/NL/lov/1996-11-29-72

Power, M.J., Desouza, K.C. & Bonifazi, C. (2006). *The outsourcing handbook. How to implement a successful outsourcing process.* London & Philadelphia: Kogan Page Limited.

Prado, E.P.V. (2011). Risk analysis in information technology and communication outsourcing. *Journal of Information Systems and Technology Management,* Vol. 8(3), pp. 605-618. DOI: 10.4301/10.4301%2FS1807-17752011000300005

PwC. (2017). *Helse Sør-Øst RHF – Ekstern gjennomgang av programmet for modernisering av IKT-infrastruktur (iMod)*. Hentet fra: https://www.helse-sorost.no/Documents/Styret/Styremøter/2017/20170628/077-2017%20Vedlegg%201%20-%20HSØ%20FY%202017%20-%20Rapport%20iMod%20v%201.0.pdf

Qi, C. & Chau, P.Y.K. (2012). Relationship, contract and IT outsourcing success: Evidence from two descriptive case studies. *Decision Support systems,* Vol. 53 (2012) pp. 859-869.

Hentet fra: http://www.dl.edi-info.ir/Relationship,%20contract%20and%20IT%20outsourcing%20success.pdf

Qi, L., Wu, H., Zhang, N. & Li, X. (2012). Risk identification and conduction model for financial institution IT outsourcing in China. *Information Technology and management,* Vol. 13 (4), pp. 429-443. DOI: 10.1007/s10799-012-0131-z

Rammeforskriften. (2001). Forskrift om helse, miljø og sikkerhet i petroleumsvirksomheten og på enkelte landanlegg m.v av 02 desember 2010. Hentet fra: https://lovdata.no/dokument/LTI/forskrift/2001-08-31-1016

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety science,* Vol. 27(2), pp. 183-213. DOI: 10.1016/S0925-7535(97)00052-0

Rausand, M. & Utne, I.B. (2009). Risikoanalyse: teori og metoder. Trondheim: Tapir akademisk forlag.

Remen, A. C. & Tomter, L. (2016). Frykter at ondsinnede utnytter «IT-nomader». *NRK.* Hentet fra: https://www.nrk.no/norge/fri-flyt-av-informasjon-kan-utnyttes-av-ondsinnede-1.12920235

Remen, A. C. & Tomter, L. (2017a). Driftet Nødnettet ulovlig fra India. *NRK.* Hentet fra: https://www.nrk.no/norge/driftet-nodnettet-ulovlig-fra-india-1.13358591

Remen, A.C. & Tomter, L. (2017b). Tastefeilen som stoppet Statoil. *NRK.* Hentet fra: https://www.nrk.no/norge/xl/tastefeilen-som-stoppet-statoil-1.13174013

Remen, A.C., Tomter, L. & Flaarønning, G. (2017). Varsler strengere Sikkerhetslov etter Nødnett-svikt. *NRK.* Hentet fra: https://www.nrk.no/norge/amundsen_-mangel-pa-risikovurdering-i-nodnett-saken-1.13798108

Renn, O. (2007). Precaution and analysis: two sides of the same coin? *EMBO reports,* Vol 8(4), pp. 303-304. DOI: 10.1038/sj.embor.7400950

Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World.* London: Earthscan.

Riksrevisjonen (2017). *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2016.* (Dokument 1, 2017-2018). Hentet fra: https://www.riksrevisjonen.no/rapporter/Documents/2017-2018/RapportOmDenArligeRevisjonOgKontrollForBudsjettaret2016.pdf

Røsjø, B. (2009). *Bør satse på datasikkerhet.* Hentet fra: https://forskning.no/olje-og-gass-bransje-petroleum-informasjonsteknologi/2009/04/bor-satse-pa-datasikkerhet

Samantra, C., Datta, S. & Mahapatra, S.S. (2013). Risk assessment in IT outsourcing using fuzzy decision-making approach: An Indian perspective. *Expert Systems with Applications*. Vol. 41(8), pp. 4010-4022. https://doi.org/10.1016/j.eswa.2013.12.024

Selvik, J, T. (2017). Risiko og sårbarhet knyttet til digitalisering i oljeindustrien. *Digi.no.* Hentet fra:https://www.digi.no/artikler/kronikk-risiko-og-sarbarhet-knyttet-til-digitalisering-i-oljeindustrien/397128

Silverman, D. (2011). *Interpeting qualitative data. A Guide to the Principles of Qualitative Research.* (4.utgave). London: Sage.

Slovic, P. (2001). The risk game. *Journal of Hazardous Materials,* Vol. 86(1-3), pp. 17-24. DOI: 10.1016/S0304-3894(01)00248-5

SINTEF. (2009). *Rammebetingelsers betydning for storulykkesrisiko og arbeids miljørisiko - En litteraturstudie.* (SINTEF A11777). Hentet fra: https://www.sintef.no/globalassets/upload/teknologi_og_samfunn/sikkerhet-og-palitelighet/rapporter/sintef-a11777-rammebetingelsers-betydning-for-storulykkesrisiko-og-arbeidsmiljorisiko---en-litteraturstudie.pdf

SINTEF. (2011). *Rammebetingelser for HMS som etableres i kontrakt : en intervjustudie.* (A19670). Hentet fra: http://evaluering.nb.no/eval-utlevering/innhold/URN:NBN:no-nb_overfortdokument_3308_Eval_0/pdf

Solli-sæther, H. (2016). Modenhet i outsourcing, offshoring og backsourcing: tilbake til fremtiden?. *Magma, 19(3),* pp. 48-56. Hentet fra: https://brage.bibsys.no/xmlui/handle/11250/2389301

Styringsforskriften. (1969). Forskrift om endring i forskrift om styring og opplysningsplikt i petroleumsvirksomheten og på enkelte landanlegg m.v av 19 juni 1969 nr. 53. Hentet fra: https://lovdata.no/dokument/LTI/forskrift/2017-12-18-2373

Tafti, M. H.A. (2005). Risks factors associated with offshore IT outsourcing. *Industrial Management & Data Systems,* Vol. 105(5), pp. 549-560. DOI: 10.1108/02635570510599940

Thagaard, T. (2013). *Systematikk og innlevelse. En innføring av kvalitativ metode.* (4. utg.). Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Tomter, L. & Remen, A.C. (2017). Millionbøter etter outsourcing av sykehus-IT. *NRK.* Hentet fra: https://www.nrk.no/norge/millionboter-etter-outsourcing-av-sykehus-it-1.13751516

Tomter, L., Remen, A.C. & Wernersen, C. (2017). Statoil henter hjem sikkerhetskritiske IT-oppgaver fra India. *NRK.* Hentet fra: https://www.nrk.no/norge/statoil-henter-hjem-sikkerhetskritiske-it-oppgaver-fra-india-1.13583173

Torjusen, A.B. (2013). IKT-sikring, en forutsetning for olje og gass HMS og anleggsintegritet. Hentet fra: https://esra.no/wp-content/uploads/2015/04/3-Torjusen.pdf

Torp, C. (2017). *Industrisamarbeid leverer retningslinje for bekjempelse av cybertrusler i olje- og gassindustrien*. Hentet fra: https://enerwe.no/dnv-gl/industrisamarbeid-leverer-retningslinje-for-bekjempelse-av-cybertrusler-i-olje-og-gassindustrien/

Van Scheers, L. (2016). Managing the risk of outsourcing the IT function at companies. *Risk Governance & Control: Financial Markets & Institutions*, Vol.6(3), pp. 69-74. DOI: 10.22495/rcgv6i3c2art9

Wei, J. & Peach, B. (2006). Development of a risk assessment model for global information technology outsourcing. *Journal of international technology and information management,* Vol. 15(4), pp 34-50. Hentet fra: http://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1180&context=jitim

Wenger, E. (1998). *Communities of practice. Learning, meaning and identity.* Cambridge: Cambridge University Press.

Willcocks, L.P. & Lacity, M.C. (1999). IT outsourcing in insurance services: risk creative contracting and business advantage. *Information systems journal, Vol 9*(3), pp. 163-180. DOI: 10.1046/j.1365-2575.1999.00061.x

Wu, R., Fung, Y. K., Feng, G. & Wang, N. (2017). Decisions making in information security outsourcing: Impact of complementary and substitutable firms. *Computers & Industrial Engineering,* Vol. 110, pp. 1–12. DOI: 10.1016/j.cie.2017.05.018

Yin, R.K. (2014). *Case study research. Design and methods.* Sage Publications, Inc: California

Vedlegg 1. *Veiledende intervjuguide operatører*

1. Fortell litt om deg selv.

Stilling, erfaring, deltakende i risikovurderingsprosessen, beslutningsmyndighet?

- Har dere outsourcet IKT-tjenester og/eller infrastruktur, og eventuelt hva? Hvorfor disse tjenestene (eventuelt alt) og ikke andre? Hvor?

2. Hvilke risikoanalyser/-metoder har dere benyttet i forbindelse med outsourcing?

- Hvordan har dere gjennomført risikovurderingsprosessen når det gjelder outsourcing? Hva har dere vurdert, og hvordan?
- Benytter dere egne metoder rettet mot informasjonssikkerhet, og eventuelt hvilke?
- Hvorfor den/de metodene, fremfor andre?

3. Hva opplever du/dere som de største risikoene/sårbarhet ved outsourcing?

- Av hvilken betydning var dette for om dere outsourcet/ikke outsourcet? Hvorfor/hvorfor ikke?
- Hvorfor ble de vektlagt, og eventuelt hvordan ble de prioritert?
- Hvordan forholder dere dere til risikoer som ikke er lett å identifisere, hackerangrep og liknende? Er dere utsatt? Hvorfor tror du /tror du ikke det er sånn?

4. Hvilke kriterier vektlegges når dere vurderer risikoen knyttet til outsourcing?

- Hvordan vektes de ulike kriteriene? Ses de opp mot standarder/interne retningslinjer, mulige tap o.l.? Hvorfor tror du det er de som vektlegges?
- Er det noen områder som anses mer relevante enn andre? (Tekniske, organisatoriske etc.) Hvorfor/Hvorfor ikke?
- Hvilke faktorer påvirker hva /hvilke kriterier dere vektlegger? Interne/eksterne krav, o.l.?

5. Er det noen ytre faktorer som påvirker risikovurderingen?

- Hvordan har risikoen blitt kommunisert videre?

- Hvordan har da eventuelt ledere forholdt seg til å akseptere/ikke akseptere risiko mener du? Hvorfor tror du det er sånn?
- Hvem er det som har besluttet om risikoen er akseptabel/ikke-akseptabel? Hvordan besluttes dette?

6. I hvilken grad har digitaliseringen av oljesektoren påvirket bedriftenes driv for outsourcing?
   (*Eksempelvis*: reduksjon i kostnader, økt fokus på kjernevirksomhet, del av bedriftens strategi, bedre tilgang til kvalifisert personell, raskere markedstilgang, nye markeder)

7. Hvilke utfordringer eller fordeler har dere sett i etterkant av outsourcingen? Eventuelt, tror du dere hadde hatt fortrinn/ulemper ved å ha hatt outsourcet?

8. Nå som dere har erfaring fra det; ville dere valgt annerledes eller er det andre kriterier dere ville vektlagt mer/mindre?

Vedlegg 2. *Veiledende intervjuguide Petroleumstilsynet*

1. Fortell litt om deg selv.

2. Hva er dine tanker rundt IKT-sikkerhet i Petroleumssektoren?
- Er lovverket tydelig nok, eller burde det vært det?

3. Hvilken rolle synes Ptil selv at dere skal ha innen IKT?

4. Når det gjelder digitale hendelser, rapporteres mye til dere? Er det tydelig nok hva som skal rapporteres generelt i sektoren? (læring)

5. Hva syns du når det gjelder læring i sektoren, når det kommer til IKT?

6. Hva tenker du rundt Ptil og tilsyn når det gjelder IKT-sikkerhet hos operatører, og deres rolle?
- Hvilken rolle tenker du evt. at Ptil skal ha?
- Er det tilstrekkelig teknisk kompetanse på området?

7. Syns du samhandlingen i sektoren er god nok når det gjelder IKT og digitale sårbarheter/hendelser? (samhandling)
- Burde det være mer samhandling, er det nok? Er det spesielle fagmiljøer å dele informasjon/lære av hverandre?

8. Hva er deres tanker rundt tilsyn på IKT-sikkerhet?

9. Har du tanker omkring NUPI & IRIS som påpeker at risikostyringen på myndighetsnivå bør forbedres?